(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2002 (21.03.2002)

PCT

(10) International Publication Number
WO 02/23904 A1

(51) International Patent Classification[7]: H04N 7/167, H04K 1/00

(21) International Application Number: PCT/US01/28348

(22) International Filing Date:
13 September 2001 (13.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/230,935 13 September 2000 (13.09.2000) US
09/816,255 26 March 2001 (26.03.2001) US

(71) Applicant *(for all designated States except US)*: **CERTIA INC.** [US/US]; 1110 Herndon Parkway, Suite 300, Herndon, VA 20170 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **HASTINGS, Paul, R., II** [US/US]; Certia Inc., 1340 Poydras Street, Suite 600, New Orleans, LA 70112 (US). **MEFFERT, Gregory, J.** [US/US]; Certia Inc., 1340 Poydras Street, Suite 600, New Orleans, LA 70112 (US).

(74) Agents: **HAMPTON, Phillip, G.** et al.; Gardner Carton & Douglas, 1301 K Street, NW, Suite 900, East Tower, Washington, DC 20005 (US).

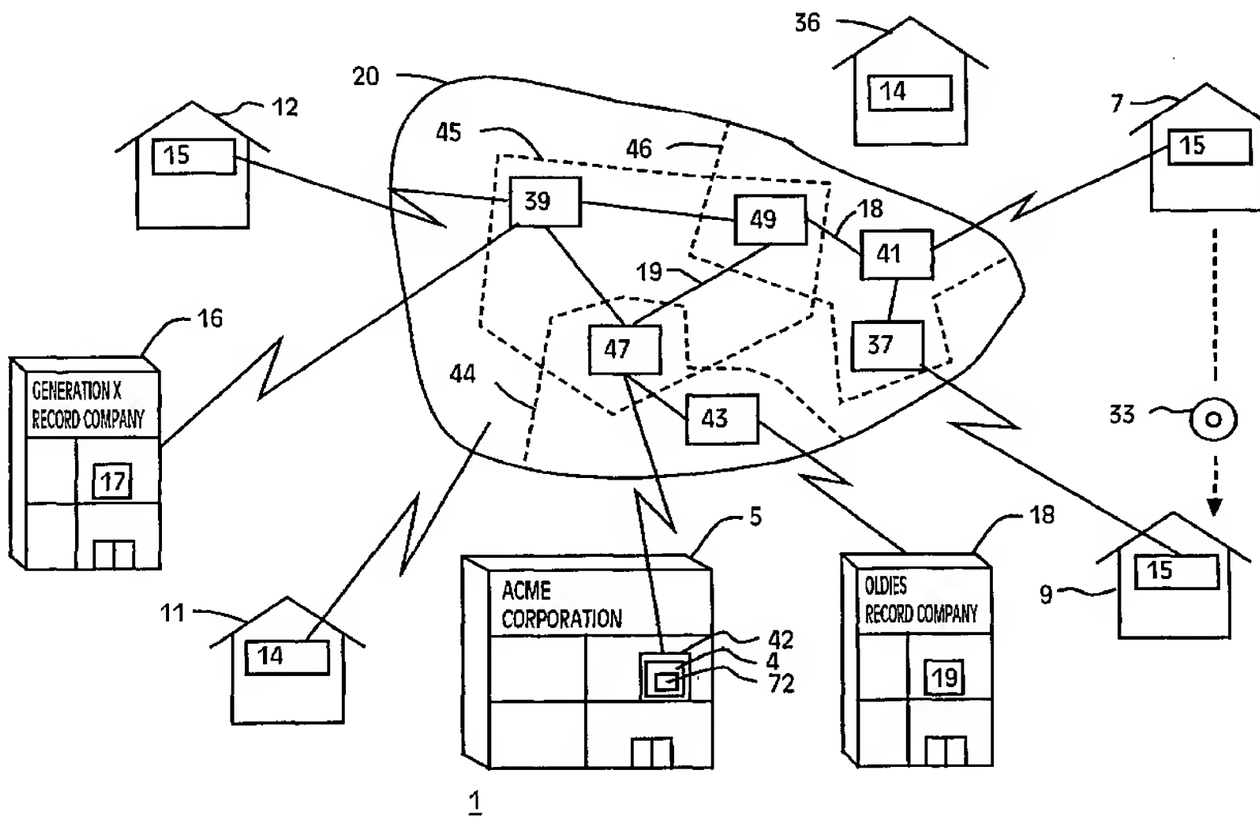
(81) Designated States *(national)*: AU, CA, IL, JP, MX, RU, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEMS AND METHODS FOR CONTROLLING USE OF CREATIVE WORKS



(57) Abstract: A system and method for controlling distribution and use of creative works. The system includes office towers (5, 16 and 18) and homes (7, 9, 11, 12 and 36). Each tower and home is connected to the global Internet (20), consisting of a plurality of nodes which may include WAN and private networks, including addresses uniquely identifying computers on the network. Each home includes apparatus for receiving and playing copies of song recordings. The digital rights manager (DRM) (1) in concert with the Content provider (17) record, sell and distribute recordings via the Intenet or portable media such as compact disks. A consumer purchases a right set form the content provider via the Internet. When the consumer plays the recording, automatic communication between the consumer's player and the contnet provider allows the consumer to exercise the rights in his possession but not to exceed those rights.

WO 02/23904 A1

SYSTEMS AND METHODS FOR CONTROLLING USE OF CREATIVE WORKS

BACKGROUND OF THE INVENTION

This Application claims the benefit of U.S. Application Serial No. 60/230,935 of Greg Meffert filed September 13, 2000 for DIGITAL RIGHTS MANAGEMENT SYSTEMS AND METHOD, the contents of which are herein incorporated by reference. This Application is a Continuation-in-Part of copending U.S. Application Serial No. 09/816,255 of Gregory J. Meffert, Donovan Mouriz, Paul R. Hastings II, Rick W. Wise and Douglas A. Laine filed March 26, 2001 for SECURED CONTENT DELIVERY SYSTEM AND METHOD.

Field of the Invention

This invention relates generally to creative works and, more particularly, to preventing unauthorized use of copies of creative works.

Description of Related Art

Unauthorized copying of creative works is an old problem.

Historically, unauthorized copying carried certain disadvantages tending to deter people. These disadvantages are fading, however. For example, an analog copy of a musical performance will have a certain amount of error. An analog copy of an analog copy will have compounded error, etc. Thus, quality degradation inherent in analog copying has been a disadvantage to making unauthorized copies. This disadvantage, however, is fading with the availability of consumer electronics that employ digital mechanisms for making a copy. Such consumer electronics include digital tape recorders and MP3 players.

Another disadvantage has been the inconvenience of obtaining hardware and a source copy to make the unauthorized copy. This disadvantage is also fading, with the universal availability of the Internet and standard formats, such as MP3, for storing content. Thus, one of the problems currently facing distribution of MPEG files is that the original owner of the content has no control of the distribution, sale, and use of the content once the files leave its control.

Some security methods for digitally encrypted content have been proposed. Many of these methods, however, may be circumvented by relatively simple manipulation of data on a consumer's machine.

Another problem with some proposed security methods is that the methods make it cumbersome for a consumer to obtain and use a legitimate copy of the content.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide improved systems and methods for controlling distribution and use of creative works.

To achieve this and other objects of the present invention, there is a method in a first system including a plurality of second systems, each second system having a respective identification signal different from the identification signal in the other second systems. The method comprises the steps, performed in each second system, of receiving a first signal; generating a second signal by encrypting using the identification signal, the second signal corresponding to the first signal; generating a third signal responsive to the second signal, by decrypting using the identification signal; and conditionally sending the first signal to an output device, depending on the third signal.

According to another aspect of the present invention, a first system comprises a plurality of second systems, each second system including a respective identification signal different from the identification signal in the other second systems; communication hardware that receives a first signal; a signal generator that generates a second signal by encrypting using the identification signal, the second signal corresponding to the first signal; a memory that stores the second signal; a signal generator that reads from the memory to generate a third signal responsive to the second signal, by decrypting using the identification signal; and logic that determines whether to send the first signal to an output device, depending on the third signal.

According to yet another aspect of the present invention, first system comprising a plurality of second systems, each second system including a respective identification signal different from the identification signal in the other second systems;
means for receiving a first signal; means for generating a second signal by encrypting using the identification signal, the second signal corresponding to the first signal;

means for generating a third signal responsive to the second signal, by decrypting using the identification signal; and means for determining whether to send the first signal to an output device, depending on the third signal.

According to yet another aspect of the present invention, there is a method in a system including a first signal containing a work, a second signal including a portion of the first signal, and a third signal including an encrypted portion of the first signal. The method comprises sending a signal to a first output device, by decrypting the third signal; and the following steps, performed in response to an action by a first consumer, sending the second and third signals to a second consumer, and the following steps, performed in response to an action by the second consumer, conditionally inhibiting the following step, responsive to a fourth signal; sending a signal to a second output device, by processing the second signal; and updating the fourth signal, responsive to the previous step.

According to yet another aspect of the present invention, there is a system for operating with a first signal containing a work, a second signal including a portion of the first signal, and a third signal including an encrypted portion of the first signal. The system comprises first circuitry that acts to send a signal to a first output device, by decrypting the third signal; and second circuitry including logic to send a signal to a second output device, by processing the second signal, logic to update a fourth signal in response to the logic to send, and logic to conditionally inhibiting the logic to send, responsive to a fourth signal.

According to yet another aspect of the present invention, there is a system for operating with a first signal containing a work, a second signal including a portion of the first signal, and a third signal including an encrypted portion of the first signal. The system comprises means for sending a signal to a first output device, by decrypting the third signal; means for sending the second and third signals from a first consumer to a second consumer; means for conditionally inhibiting the following means, responsive to a fourth signal; means for sending a signal to a second output device, by processing the second signal; and means for updating the fourth signal, responsive to the previous means.

According to yet another aspect of the present invention, there is a method in a system including a plurality of first systems, each first system configured to process a file, a plurality of second systems, each second system configured to process a file. The method comprises generating a file having a first part decodable by one of the first systems or second systems, a second part decodable by one of the second systems using a first

decryption key, and a third part decodable by one of the second systems without using the first decryption key.

According to yet another aspect of the present invention, there is a method for a system having a program having a first instruction set that selects a file responsive to a signal from an input device, and a second instruction set that processes a portion of the selected file for sending to an output device, wherein the first instruction set passes control to the second instruction set, responsive to a content of a data structure. The method comprises replacing the second instruction set with a third instruction set by setting the content of the data structure to include a direction to the third instruction set, the third instruction set acting to receive the portion of the selected file and decrypt the portion responsive to a decryption key.

According to yet another aspect of the present invention, there is a method comprising the steps, performed for a first consumer, of processing a first signal; and sending a signal to a first output device, responsive to the previous step. The method also comprises the steps, performed for the second consumer, of receiving the first signal from the first consumer via a first signal path; receiving a first key via a second signal path; processing the first signal using the first key; and sending a signal to a second output device, responsive to the previous step.

According to yet another aspect of the present invention, there is a system comprising a first system including a first output device; a processor that processes the first signal to generate a first processed signal; a sender that sends the first processed signal to the first output device. The system also includes a second system having a second output device; communication hardware that acts to receive the first signal via a first signal path, and receive a first key via a second signal path; a processor that processes the first signal, using the first key, to generate a second processed signal; a sender that sends the second processed signal to the second output device, wherein the first system includes communication hardware that sends the first signal to the second system.

According to yet another aspect of the present invention, a system comprises first means for processing a first signal; means for sending a signal to a first output device, responsive to the previous means; means for receiving the first signal from the first means for processing via a first signal path; means for receiving a first key via a second signal

path; second means for processing the received first signal using the first key; and means for sending a signal to a second output device, responsive to the previous means.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a diagram showing an overview of an exemplary system 1, in accordance with a first preferred embodiment of the present invention.

Figs. 2A and 2B are a data flow diagram for describing a data encrypting process in system 1.

Fig. 3 is a diagram of a data structure generated by the process shown in Figs. 2A and 2B.

Fig. 4 is a diagram emphasizing a portion of the data structure shown in Fig. 3.

Fig. 5 is a flow chart for describing a process performed in system 1.

Fig. 6 is a diagram showing circuitry in a consumer's home.

Fig. 7 is a diagram emphasizing aspects of the circuitry shown in Fig. 6.

Fig. 8. is a flow chart of a process performed in system 1.

Fig. 9. is a diagram showing circuitry in another consumer's home.

Fig. 10 is a diagram emphasizing a portion of the circuitry shown in Fig. 9.

Fig. 11 is a diagram showing circuitry in another consumer's home.

Fig. 12 is a diagram emphasizing a portion of the circuitry shown in Fig. 11.

Fig. 13 is a diagram showing an overview of another exemplary system in accordance with a second preferred embodiment of the present invention.

Figs. 14A and 14B are a data flow diagram for describing a process in system 2.

Fig. 15 is a diagram of a data structure generated by the process shown in Fig. 14A and 14B.

Fig. 16 is a diagram of circuitry in a consumer's home.

Fig. 17 is a diagram emphasizing a portion of the circuitry shown in Fig. 16.

The accompanying drawings, which are incorporated in and which constitute a part of this specification, illustrate embodiments of the invention. Throughout the drawings, corresponding parts are labeled with corresponding reference numbers.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

First Preferred Embodiment

Fig. 1 shows system 1 for controlling distribution and use of copies of song recordings in accordance with a first preferred embodiment of the present invention. System 1 includes office towers 5, 16, and 18; and homes 7, 9, 11, 12, and 36. Office towers 5, 16, and 18; and homes 7, 9, 11, 12, and 36 are separate buildings. These buildings are widely separated geographically. For example, tower 5 is in Nashville, Tennessee; home 7 is in Los Angeles California; and home 9 is in Honolulu, Hawaii. Some of these buildings could be in countries other than the United States.

Each of tower 5, tower 16, tower 18, home 7, home 9, home 11, and home 12 is connected to the global Internet 120.

Tower 16 houses content provider 17, and tower 18 houses content provider 19.

Tower 5 houses computer 42.

Each of homes 7, 9, and 12 includes a respective circuitry 15 for receiving and playing copies of song recordings. Circuitry 15 can play audio files in MPEG layer 3 (MP3) format. Circuitry 15 can also play files in a format generated by Acme Corporation, as described below. In this Patent Application, the word circuitry encompasses dedicated hardware, and/or programmable hardware, such as a central processing unit (CPU) or reconfigurable logic array, in combination with programming data, such as sequentially fetched CPU instructions or programming data for a reconfigurable array.

Each of homes 11 and 36 includes a respective circuitry 14 for receiving and playing copies of song recordings. Circuitry 14 can play files in the MP3 format. Circuitry 14, however, cannot play files in the Acme Format.

In global Internet 20, network 44 includes a plurality of nodes, including computer 42, computer 43, and computer 47, each having a respective network address uniquely identifying the computer on network 44. Network 45 includes a plurality of nodes, including computers 47, 39, and 49, each having a respective network address uniquely identifying the computer on network 45. Network 46 includes a plurality of nodes, including computer 49, 41, and 37, each having a respective network address uniquely identifying the computer on network 46. Computer 49 exchanges data with computer 41 via wide area network (WAN) communication link 18. Computer 49 exchanges data with computer 47 via WAN communication link 19.

Disk 33 is a type of portable medium that a consumer, residing in home 7, uses to send a file to a consumer, residing in home 9. Disk 33 may be an optical disk or a magnetic disk, for example.

Computer 42 includes hardware executing software to effect server 4.

Formatting of Content for Distribution to Consumers

Server 4 includes COM object 72, accessible through active server pages on Internet 20.

COM object 72 includes interfaces that allow clients access to COM object 72. Such clients include content provider 17 in tower 16 and content provider 19 in tower 18.

COM object 72 makes calls to a Java-based encryption engine through the JNI interface provided by Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, CA 94303.

Acme Corporation is the digital rights manager (DRM) that operates server 4. Content provider 17 acting in concert with Acme Corporation encrypts a recording of a song and distributes the recording via a media distribution channel such as Internet 20 or portable media such as compact disks. Associated with the encrypted recording are several sets of rights each of which governs how the recording may be used. A consumer may buy a rights set from content provider 17, via Internet 20 for example. When the consumer invokes his personal consumer electronics to play the recording, automatic communication between the consumer's personal electronics and Acme Corporation may ensure that the consumer may exercise the rights in his possession but not exceed the rights in his possession.

A first consumer may send a copy of the recording to another consumer. System 1, however, preempts the first consumer from effectively sending a copy of his rights to the other consumer 161.

Figs. 2A and 2B are a data flow diagram for describing a process performed in system 1, and Fig. 3 is a diagram emphasizing aspects of a file 136 produced by the process. Performer 22 generates acoustic signal 23. Microphone 24 receives acoustic signal 23, translates the acoustic signal 23 into an electrical signal, and sends the electrical signal to analog-to-digital encoder 26, which generates digital song file 106. Formatter, 28

receives file 106 and generates a file 108 in MP3 format. In this example, file 108 is in the possession of content provider 17.

Content provider 17 sends file 108 to server 4 in Acme Corporation. Content provider 17 also sends data defining four sets of rights to the sound recorded in file 108. The first set of rights includes the right to play the song for an unlimited amount of time, and the right to distribute the song to others. The second set includes the right to play the entire song an unlimited amount of time. The third set includes the right to play the entire song a limited number of times. The fourth set includes the right to play a portion of the song for a limited number of times.

Server 4 receives file 108 from content provider 17, and data defining the four rights sets from content provider 17, to generate file 136.

More specifically, server 4 includes instructions 34 executed by a CPU. Instructions 34 act to generate file 136 containing encrypted audio data.

Instructions 34 act to generate 4 pairs of keys. Instructions 34 generates a respective key pair for each rights set. A first key pair includes public key 168 and private key 158. A second key pair includes public key 167 and private key 157. A third key pair includes public key 166 and private key 156. A fourth key pair includes public key 165 and private key 155.

Server 4 first generates two symmetric keys, one (symmetric key A) that will be used to encrypt the trial portion of the song (i.e. the first 30 seconds), and one (symmetric key B) that will be used to encrypt the remainder of the song. Server 4 then uses public keys 166, 167, and 168 to encrypt (envelope) symmetric key B, and public key 165 to encrypt symmetric key A.

Since Public keys 166, 167, and 168 all encrypted the same symmetric key (symmetric key B), any one of their corresponding private keys (156, 157, or 158) may be used to decrypt symmetric key B. Since symmetric key B was used to encrypt the primary (non-trial) portion of the audio, the private keys 156, 157, and 158 enable the possessor of such keys to obtain access to the un-encrypted primary audio.

Similarly, since Public key 165 was used to encrypt symmetric key A, its corresponding private key (155) may be used to decrypt symmetric key A. Since symmetric key A was used to encrypt the trial portion of the audio, private key 155 enables the possessor of such key to obtain access to the un-encrypted trial audio.

Server 4 generates file 136 to include public keys 168, 167, 166, and 165. Within file 136, each of public keys 168, 167, 166, and 165 is enclosed within a respective digital certificate, formatted in the X.509 standard.

Server 4 embeds unencrypted audio field 114 into a common file 136 with cipher data 125 and 127. Field 114 includes a set of standard MP3 frames, synchronized according to the MP3 standard. Field 114 includes a prerecorded voice saying "This is an Acme protected MP3 file. To obtain software or rights to play this file, please go to http://music.acme.com." This prerecorded voice message can be played on conventional MP3 players (circuitry 14), as well as circuitry 15 that can play Acme-formatted files.

A related aspect of the Acme format is "desynchronization" of fields subsequent to field 114, meaning that these subsequent fields will not play on conventional MP3 players. Field 114 is not desynchronized. Thus, a conventional MP3 player, which cannot decrypt Acme-encrypted data, will only attempt to play message 114. This "graceful failure" mechanism allows recipients of the Acme-formatted media to obtain the appropriate software to access the media, without hearing garbled audio.

To desynchronize, ensuring that data 125 and 127 do not play as garbled audio in conventional MP3 players, server 4 removes certain bit patterns from data 125 and 127. Server 4 replaces "11111111 111 x x x x x" patterns, in data 125 and 127, with "11111111 00000000 111 x x x x x" , and "11111111 00000000" patterns with "11111111 00000000 00000000", wherein "x" denotes either a "0" or a "1".

In generating file 136, server 4 preserves the MP3 characteristics of input file 108. Server 4 generates file 136 such that any pre-audio data, such as ID3v2 tags and any post-audio data, such as the 128-byte TAG that often appears at the end of MP3 files, in file 108 also appear in the file 136.

File 136 includes cipher data 125 for allowing 30 second trial play. To allow distribution and some use of file 136 without involving Acme Corporation server 4, generates files 136 to include trial key 155. Cipher data 125 may be decrypted with trial key 155. Trial key 155, however, cannot be used to decrypt the remainder of the song encrypted in cipher data 127. Thus, the song may be effectively unlocked for the first 30 seconds during trial play, while the remainder of the song is locked with a public key corresponding to a secured rights set.

Server 4 sends file 136, including private key 155, back to the content provider. Server 4 also sends privates keys 158, 157, and 156 back to the content provider. Server 4

may send private keys 158, 157, and 156 back to the content provider at the time of sending file 136. Alternately, Acme Corporation may store private keys 158, 157, and 156 for the content provider, and send one of these private keys in response to later requests from the content provider. This latter approach relieves the content provider of much of the security-related processing involved with storing private keys. Under this latter approach, a consumer may purchase a particular set of rights by communicating with the content provider over Internet 20 and, in response to this communication from the consumer, the content provider would request the corresponding private key from Acme Corporation and immediately relay the private key to the consumer, without long term storage of the private key within the content provider.

When sending a private key to a consumer, content provider uses a Secure Socket Layer (SSL) link in Internet 20.

The respective data in each of files 106, 108, and 136 is a type of signal.

Fig. 4 is a simplified diagram showing some of the fields in file 136. Pre-audio data 112 includes ID3v2 data if present. Fields 125 and 127 are encrypted. Index field 121 is a table of offsets to subsequent fields in file 136. Post audio data 134 includes a 128 byte tag.

Fig. 4 shows some of data field 123 in more detail. Data field 123 includes a respective X.509 digital certificate for each set of rights that may apply to file 136. Each of private key 155, 156, 157, and 158 corresponds to a respective one of certificates 185, 186, 187, and 188. To implement the functionality described above, respective digital certificates represent respective rights sets.

File 136 is one type of data structure for associating the fields of file 136 with each other.

Player software 142 in home 7 (Fig. 6) tries to match one of certificates 188, 187, or 186 shown in Fig. 4. More specifically, key database 141 is a secure certificate/private-key store. Records in database 141 are accessed by a certificate issuer name-serial number pair. Record 59 includes the certificate for the song (work) in file 139. Records 60 include respective certificates for other works in other files.

Software 144 attempts to access certificates with "higher" rights levels, which appear before keys with lower rights levels. Thus, when software 144 checks key database 141 for a key to decrypt a particular piece of media, it will encounter any

ownership-distribution key before encountering any limited use key. Software 142 searches database 141 for certificate 188 and if the search finds certificate 188, and the corresponding private key 158, certificate 188 is considered to be the matching certificate. If certificate 188 is not the matching certificate, software 142 searches database 141 for certificate 187 and if the search finds certificate 187, and the corresponding private key 157, certificate 187 is considered to be the matching certificate. If neither certificate 188 nor certificate 187 is the matching certificate, software 142 searches database 141 for certificate 186 and if the search finds certificate 186, and the corresponding private key 156, certificate 186 is considered to be the matching certificate.

Software 142 uses any private key, found with the method described in the previous paragraph, to decrypt cipher data 127. More specifically, software 142 uses any private key, found with the method, to decrypt a symmetric key, and then uses the decrypted symmetric key to decrypt the cipher data 127.

Trial rights certificate 185 includes field 85 storing a code indicating that cipher data 125 may be played a certain number of times. Play rights certificate 186 includes field 86 storing a code indicating that cipher data 125 and cipher data 127 may be played a controlled number of times, the controlled number being stored in a log record at the time of play purchase. Owner rights certificate 187 includes field 87 storing a code indicating that cipher data 125 and cipher data 127 may be played an unlimited number of times. Owner-distribution rights certificate 188 includes field 88 storing a code indicating that cipher data 125 and cipher data 127 may be played an unlimited number of times, and that the consumer may send file 136 to another consumer.

Each of certificate 188, 187, 186, and 185 includes a Subject Name, that is a Distinguished Name, identifying the work in file 136. The identification information includes a name for the work, performer, and performance date. The work may be a song or an album of songs, for example.

Thus, possession of a certificate and private key, in key database 141, allows player software 142 to effect a set of rights for a particular work.

Cipher data 125 is encrypted with a first symmetric key. Field 123, includes an encrypted version 175 of the first symmetric key, the encrypted version 175 being encrypted with key 165, and decryptable (able to be decrypted) with trial key 155.

Cipher data 127 is encrypted with a second symmetric key. Field 123, includes an encrypted version 176 of the second symmetric key, the encrypted version 176 being encrypted with key 166, and decryptable with limited use key 156. Field 123, includes an encrypted version 177 of the symmetric key, the encrypted version 177 being encrypted with 167, and decryptable with ownership key 157. Field 123, includes an encrypted version 178 of the symmetric key, the encrypted version 178 being encrypted with key 168, and decryptable with distribution key 158.

Fig. 5 is a flow chart showing a process performed by the circuitry shown in Figs. 2A and 2B. The left column of Fig. 5 shows steps performed by a content provider, such as provider 17, while the right column shows steps performed by Acme Corporation.

The content provider obtains or creates a work, stored in song file 106. (Step 5).The content provider establishes rights sets (step 10) to describe allowable usage for their media. Acme Corporation performs acts for enforcement of rights and for allowing no more usage than that dictated by the content provider.

The content provider sends the media and data defining the rights sets to Acme Corporation (Step 15). Server 4, operated by Acme corporation, identifies and processes the content file (Step 20), creates a respective pair of keys for each rights set (Step 25), creates a file containing unencrypted message 114 (Step 30), and creates cipher data 127 (Step 35).

Server 4 sends file 136 back to content provider 17 (Step 40), and sends private keys 155, 156, 157, and 158 to content provider 17 (Step 45).

Private keys 158, 157, and 156 are not stored in the file 136. Public keys 165, 167, 166, and 165, embedded in respective X.509 certificates, are stored in file 136.

Content provider 17 then collects the resultant protected file 136 and keys 156, 157, and 158 for respective distribution and sale.

Because system 1 now protects file 136, the content provider is free to distribute file 136 by any available traditional or new channels.

The consumer is free to distribute file 136 to his contacts to enhance distribution. In this sense, the process is the same as distribution by the content provider.

Processing of Formatted Content to Play Music for a Primary Consumer

Fig. 6 shows circuitry 15 in home 7. Circuitry 15 includes a personal computer (PC) having CPU 135, and memory 153 for storing programs and data. Memory 153 includes random access memory (RAM) and disk memory. Various parts of programs and data in RAM may be transferred between RAM and disk memory using a virtual memory mapping scheme, as is well known in the art.

Circuitry 15 also includes CRT display 158, mouse input device 159, keyboard input device161, and telecommunications hardware 157, which may include a modem, PSTN interface circuitry, T1 interface circuitry, or wireless transceiver, for example.

Conventional Internet software 138, such as Netscape Communicator™, receives file 136 from content provider 17 via Internet 20 and hardware 157.

Player software 142 processes a file to send a signal from the file to sound card 70. Sound card 70, responsive to the signal from software 142, sends audio signals to speakers in headphones 68. Each speaker in headphone 68 is a type of transducer

Player software 142 selects file 136 or one of files 137 for playing. More specifically, player software 142 displays a file selection menu on CRT158 and then selects a file responsive to a signal from mouse 159 or keyboard 161.

If the selected file is in the Acme format, software 142 acts to resynchronize the file fields that were desychronized by server 4 in a process described above. In other words, software 142 restores the bit patterns that were removed by server 4.

Machine ID 126 is unique to the particular circuitry 15 in home 7. ID 126 is a Global Unique Identifier (GUID) or Universal Unique Identifier (UUID), which is a unique number. ID 126 may be stored in the system basic input/output system (BIOS) of the PC, for example.

In other words, machine ID 126 is different from each of machine ID 126 in circuitry 15 in home 9, machine ID 126 in circuitry 15 in home 11, machine ID 126 in circuitry 15 in home 12, and machine ID 126 in circuitry 15 in home 36.

Fig. 7 shows player software 142 in more detail. Software 144 detects whether the file is an encrypted or standard MP3 file and also determines basic audio stream characteristics necessary for rendering the stream (such as sampling rate, frequency, etc.). Software 146 decrypts the audio content and renders the audio with the basic parameters retrieved from software 144.

Software 142 includes audio software 199, which is a Real Player™ supplied by RealNetworks, Inc., PO Box 91123, Seattle, WA 98111. Audio software 199 invokes management software 144 via the Real Player "file format plug-in" interface table entry 203; table entry 203 contains location information for a program to be executed when execution thread 201 is passing control to the file format plug-in. In other words, execution thread 201 passes control to a program dictated by the contents of table entry 203.

Programs invoked via a Real Player plug-in interface are Dynamic Link Library (DLL) files.

More specifically, execution thread 201 in player 199 passes control via the File Format plug-in interface depending on the media MIME (Multipurpose Internet Mail Extension) type, determined by the media's file extensions (in this case, MP3). When player 199 starts, an initialization section 200, of execution thread 201, searches for plug-ins in the subdirectory named plug-in below the directory in which player 199 resides. In the example of Fig. 7, this subdirectory is subdirectory 202.

Initialization section 200 examines executable files in subdirectory 202 to find an executable file identified as being for MP3 file format and, upon finding such a file, sets entry 203 with location information for the file. In Fig. 7, a file containing software 144 is the only file in subdirectory 202 identified as being for MP3 file format. Thus, initialization section 200 sets entry 203 with location information for software 144.

Audio software 199 invokes decryption software 146 via the Real Player "rendering plug-in" interface table entry 205; table entry 205 contains location information for a program to be executed when execution thread 201 is passing control to the rendering plug-in.

Initialization section 200 examines executable files in subdirectory 202 to find an executable file identified as being for MP3 file rendering and, upon finding such a file, sets entry 205 with location information for the file. In Fig. 7, a file containing software 146 is the only file in subdirectory 202 identified as being for MP3 file rendering. Thus, initialization section 200 sets entry 205 with location information for software 146.

With software 144 installed as a file format plug-in in subdirectory 202, and software 146 installed as a rendering plug-in in subdirectory 202, player 199, software 144, and software 146 may be considered a common program. The instructions in this common program, excluding software 146, act to select file 136 or one of files 137 for playing.

Software 144 initializes Real Network's "Audio Services" before software 146 has data to stream. To enable this initialization, software 144 extracts some basic audio information from file 136. Thus, both software 144 and software 146 use a common decryption program. Software 144 determines if the input file is Acme-encrypted or, instead, is the conventional standard MP3 data. Software 144 determines the audio sampling parameters (sampling frequency, number of audio channels, bit-rate, etc). Software 144 determines if sufficient rights exist for file 136 to be played.

Software 144 reads raw data from the file system, via the File System Plug-in, and packets the data. Software 144 then sends the packets of data to software 146 where the packets are decrypted and sent to Real Audio's "Audio Services" for playback; software 144 packetizes encrypted data, and a software 146 decrypts the data before it handles the MP3 decoding.

Software 144 sends cipher data 125 to decryption software 146, in encrypted form. Software 146 uses a key from database 141 to decrypt cipher data 125 and generate audio data for sending to headphones 68, via sound card 70.

Depending on whether an appropriate key is present in key database 141, management software 144 sends cipher data 127 to decryption software 146, in encrypted form. Decryption software 146 uses a key from key database 141 to decrypt cipher data 127 and generate audio data for sending to headphones 68, via sound card 70.

Depending on the type of key in key database 141, software 144 may create and modify records in log file 148, to limit the number of plays of cipher data 125 or 127 of file 136.

If none of keys 158, 157, or 156 are present in key database 141, software 144 uses trial key 155, embedded in file 136.

If software 144 determines that access to the file is denied, software 144 streams unencrypted informational message 114 (Fig. 3) to software 146. If the input file is not Acme-encrypted, software 144 streams the entire file to software 146, and sets appropriate flags via Stream headers to indicate a non-Acme-encrypted file.

Software 144 interacts with software 146 only through the state machine intrinsic to player 199 itself. Thus, no logical memory can be copied from one plug-in to another without player 199's state machine.

Software 146 effects decryption through RSA Java library calls (made through Sun's JNI interface).

While decryption of Acme-encrypted data is performed in software 146, translation of compressed MP3 audio date into Pulse Code Modulation data, that PC sound card 70 can render, is based on publicly available source code. The source includes the "Amp 11" Mpeg player distributed under GNU license. The Amp 11 decoding engine (which itself was based on Fraunhofer's audio compression techniques) is modified to handle streaming media.

Except for the decryption engine, both software 144 and software 146 are written in C++.

Fig. 8 is a flow chart showing a process in system 1. After installing software 144 and software 146 plug-ins, a consumer is free to play Acme-encrypted media. When a consumer selects a file for playing, software 144 initializes. Software 144 validates the integrity of software 144 to ensure that no tampering has occurred with its instructions. (step 5). Software 144 validates its integrity by calculating a digest (redundancy code), using the SHA-1 algorithm, for instructions in software 144. This digest is then compared to the decrypted digital signature of the signed code module for software 144. If tampering has occurred, software 144 disallows future access for protected components.

Software 144 checks for the existence of a record corresponding to file 136 in log file 148. (Step 10). If such a record exists in log file 148 (Step 15), software 144 examines usage right in the record (Step 25). If such a record does not exist, software 144 creates a record and assigns trial rights (Step 20).

If rights are not available for the media to be played, software 144 only allows playing of the unencrypted audio segment 114 (step 37). If rights are available, software 144 fetches an encryption key from key database 141 (step 35), updates usage information in the record in log file 148 (step 40), and instructs software 146 (step 45) to play the media or media segment for which rights exist locally.

A plurality of files 137 include respective Acme-encrypted works.

Records in log file 148 are accessed by identification information for the work. More specifically, the access data for records in file 148 is the same as the subject name of the digital certificate for the work.

The consumer may, using Internet 20, purchase rights sets from the content provider. To complete the purchase transaction, the content provider sends the consumer a few kilobytes of information, including the private key corresponding to the purchased rights set.

Processing of Formatted Content to Play Music for a Secondary Consumer

Software 138 in home 7 allows consumer 150 to forward a copy of file 136 to a friend in home 12, by attaching file 136 to an electronic mail message and sending the electronic mail message via hardware 157.

Fig. 9 shows circuitry, including player software 142 in home 12, and Fig. 10 shows player software 142 in home 12 in more detail.

When consumer 161 activates mouse 159 to request a play of file 136 received from home 7, software 144 searches key database 141 for ownership-distribution key 158, by searching for ownership-distribution certificate 188 in database 141. If, as in the example of Figs. 9 and 10, software 144 does not find a ownership-distribution key 158 in database 141, software 144 searches key database 141 for ownership key 157. If, software 144 does not find a ownership key 157 in database 141, software 144 searches key database 141 for play key 156. If software 144 does not find play key 156 in database 141, software 144 uses trial key 155 embedded in 136.

Software 144 searches log file 148 for a record for file 136. Records in log file 148 are accessed by identification information for the work. Record 180 is for the song (work) in file 139. Respective records 62 are for respective other works in other files that have been processed by software 142 in home 12.

If no such record is found, software 144 creates a file 148 record for the work to be played, and uses rights data from any matching certificate to initialize the file 148 record. In the example of Figs. 9 and 10 where there is not a matching certificate in database 141, software 144 copies a play count from rights data 85, in trial certificate 185, into field 181 in record 180, to track the number of times that the song of file 136 may be played on a trial basis.

Software 144 compares the count field 181 of the file 148 record 180. If the count field is greater than 0, software 144 decrements the count field, and plays the song. If the count field is 0, software 144 inhibits the playing of the song, and the unencrypted informational message 114 is played so that the user is instructed how to obtain rights to play the song.

Software 144 creates a hash (message digest) of log file 148 and signs the hash to create an encrypted hash 149. The hash is one type of redundancy code.

Software 144 signs the hash with a key derived from machine ID 126. In other words, software 144 uses machine ID 126 to sign the hash.

Thus, on subsequent accesses of log file 148, software 144 reads and verifies encrypted hash 149 to detect unauthorized attempts to alter file 148. Such unauthorized attempts will affect the value for encrypted hash 149, resulting in draconian reaction by the software 144 (i.e., removal of all rights, etc.).

To secure log file 148 from indirect tampering (i.e., backup and restore operations), software 144 copies encrypted hash 149 to storage location 151 and 153. Software 144 writes encrypted hash data 151 in a portion of the disk separate from that used to store log file 148. For additional security software 144 writes encrypted hash data 153 in another separate location on the disk. Thus, attempts to restore an older log file 148 will result in draconian reaction by software 144.

To hear the entire song in file 136, consumer 161 may login to Internet 20 and register for the song, either through purchase or some promotion, thereby obtaining a play key 156, ownership key 157, or ownership-distribution key 158 to decrypt cipher data 127 in file 136.

Thus, a consumer may distribute an entire work and recipients, down stream from the consumer, can only hear the first part of the work before registering for that work via the Internet.

Software 142 maintains key database 141 in encrypted form. Software 142 encrypts key database 141 using a key derived from machine ID126. In other words, software 142 uses machine ID 126 to encrypt key database 141. Thus, protection is essentially performed on a per song basis.

A modified (hacked) plug-in will not have access to keys for all songs. Thus, even a modified plug-in cannot decrypt all secure content.

An alternative is to not encrypt the trial portion of the song, thus allowing unlimited plays of the first 30 seconds of the song.

Operation of Acme-Encoded Files with Conventional MP3 Players

Fig. 11 shows circuitry 14 in home 11, and Fig.12 emphasizes player software 192 in circuitry 14. Player software 192 is conventional Real Player software with subdirectory 202 including a file containing conventional Real Player file format plug-in software194, which is identified as being for MP3 file format. Thus, at run time initialization, player 139 sets entry 203 to contains the location information for conventional software 194.

In software 192, subdirectory 202 includes a file containing conventional Real Player rendering plug-in software196, which is identified as being for MP3 rendering.

Thus, at run time initialization, player 139 sets entry 205 to contains the location information for conventional software 196.

Home 36 includes a respective instance of circuitry 14 configured with conventional real player file format and rendering plug-ins.

As described above, both conventional circuitry 14 and circuitry 15 of the first preferred embodiment can process message field 114 to play the unencrypted audio message stored therein.

In summary, server 4 generates file 136 by encrypting a song audio data 110. Content provider 17 sends file 136 to consumer 150 operating player software 142 in home 7 via Internet 20. Player software 142 in home 7 decrypts file 136 using trial key 155 and ownership-distribution key 158. More specifically, player software 142 in home 7 decrypts cipher data 125 by using trial key 155 to decrypt encrypted symmetric key 175 in field 123, and then using the thus decrypted symmetric key to cipher data 125. Player software 142 in home 7 decrypts cipher data 127 by using ownership-distribution key 158 to decrypt encrypted symmetric key 178 in field 123, and then using the thus decrypted symmetric key to decrypt cipher data 127. With this decrypting, software 142 and sound card 70 act to send an analog audio signal to headphone 68 in home 7 .

Later, consumer 150 invokes Internet software 138 to send file 136 to consumer 161 in home 12, via Internet 20. Consumer 150 thus sends file 136, without sending ownership-distribution key 158. Key 158 cannot be effectively transferred from one machine to another because key 158 is encrypted with a symmetric key that is derived from machine ID 126.

When consumer 161 in home 12 invokes player software 142, player software 142 searches for keys 158, 157, or 156 in key database 141. In this example, keys 158, 157, or 156 are absent from key database 141 in home 12. Thus, player software 142 uses trial key 155.

Player software 142 in home 12 decrypts a portion of file 136 using trial key 155. More specifically, player software 142 in home 12 decrypts cipher data 125 by using trial key 155 to decrypt encrypted symmetric key 175 in cipher data 125, and then using the thus decrypted symmetric key to decrypt cipher data 125. With this decrypting, software 142 and sound card 70 act to send an analog audio signal to headphone 68 in home 12 .

If consumer 161 purchases ownership key 157, for example, circuitry 15 in home 12 receives ownership key 157 via a signal path through Internet 20 that is different from the signal path used to receive file 136 from home 7.

Server 4 generates file 136 having unencrypted field 114 playable by circuitry 14 or circuitry 15, cypher data 127 playable by circuitry 15 using a key 158, 157, or 156, and cypher data 125 playable by circuitry 15 without using any of keys 158, 157, or 156.

Consumer 150 may send a copy of file 136 to a consumer in home 9, via portable disk 33. The consumer in home 9 may then use the file 136, subject to the safeguards and conditional controls described in connection with consumers 150 and 161.

Consumers may use various other types of devices - including portable, dedicated compact disk players - to play Acme-encrypted files, subject to the safeguards and conditional controls described in connection with circuitry 15.

Program 192 may be modified to generate program 142. The parts of program 192 excluding rendering plug-in 196 may be considered a first instruction set that selects a file, such as file 136, responsive to a signal from an input device, such as (mouse 159). Rendering Plug-in 196 may be considered a second instruction set that processes the selected file for sending to headphones 68.

The modification method includes replacing plug-in 196 with plug-in 146 acting to receive the selected file and decrypt a portion responsive to a decryption key. This replacement includes removing, from subdirectory 202, the file containing software 196; and inserting, into subdirectory 202, a file containing software 146.

The modification method also includes replacing plug-in 194 with plug-in 144. This replacement includes removing, from subdirectory 202, the file containing software 194; and inserting, into subdirectory 202, a file containing software 144.

Second Preferred Embodiment

Fig. 13 shows system 2 for controlling distribution and use of copies of written works, such as novels or journal articles. System 2 includes office tower 205; and homes 7, 9, and 12.

Each of tower 205, home 7, home 9, and home 12 is connected to the global Internet 120.

Tower 205 is operated by the Beta Publishing Corporation. The Beta Publishing Corporation is a provider of content of books and periodicals. Tower 205 houses computer 242. Computer 242 includes hardware executing software to effect server 204.

Each of homes 7, 9, and 12 includes circuitry 215 for receiving and displaying a copy of a written work.

Formatting of Content for Distribution to Consumers

Figs. 14A and 14B are a data flow diagram for describing a process performed in system 2, and Fig. 15 is a diagram emphasizing aspects of a file produced by the process. Author 222 types on keyboard 161 to record her novel. Personal computer 226, responsive to signals from 161, generates text file 206 in WordPerfect format. Formatter 228 receives file 206 and generates a file 208 in Adobe™ portable document format (PDF).

Beta Publishing Corporation receives a novel in either file 206 or 208. Server 204 in Beta Publishing Corporation generates 2 key pairs.

A first key pair includes public key 265 and private key 255. Server 204 inserts both public key 265 and private key 155 into file 236. Private key 255 allows a consumer to read the first chapter of the novel without having to purchase a key for reading the remainder of the novel.

Server 204 generates a second key pair including public key 268 and private key 258.

Server 204 uses public key 268 to encrypt most of the novel. Private key 258 may be used to decrypt the part encrypted with key 268.

Server 204 uses public key 265 to encrypt the first chapter of the novel.

Server 204 embeds unencrypted message 214 into a common file 236 with cipher data 225 and 227. Data 224 includes text stating "This is a Beta protected PDF file. To obtain software or rights to read this file, please go to http://beta.com." Thus, file 236 will fail gracefully if used with Adobe readers that do not support the encrypted format of Beta Corporation.

File 136 includes cipher data 225 for viewing the first chapter of the novel. To allow distribution and conditional use of file 236 without involving Beta Corporation computers, server 204, generates files 236 to include trial key 255. Cipher data 225 may be decrypted with trial key 225. Trial key 225, however, cannot be used to decrypt the remainder of the novel in cipher data 227.

Fig. 16 shows circuitry 215 in home 7. Circuitry 215 includes a personal computer (PC) having CPU 135, and memory 153 for storing programs and data.

Conventional Internet software 138, such as Netscape Communicator™, receives file 236 from Beta Corporation via Internet 20 and hardware 157.

Reader software 242 processes file 236 to send a signal to CRT 158. CRT 158, responsive to the signal from software 242. Displays a light signal for perception by consumer 150.

Fig. 17 shows reader software 242 in more detail. Software 242 includes instructions 239 to effect the functionality of an Adobe PDF file reader combined with the functionality for processing and encrypting portions of key database 141 and log file 148, as described in connection with the first preferred system above.

The consumer may, using Internet 20, purchase private key 268 from Beta Publishing Corporation.

Conclusion

Thus, systems 1 and 2 allow mechanisms by which a person with either basic or enhanced rights for a piece of digital property may transmit that property to a person or system with either a reduced set of rights or no rights without compromising rights enforcement. By example, a person who owns an Acme-encrypted MP3 file could give that file to a friend, and that friend could play the MP3 file with reduced rights. Systems 1 and 2 thus provide processing of conditional use rights without involving an on-line connection to a content provider or other control agent.

Additional advantages and modifications will readily occur to those skilled in the art. The invention in its broader aspects is therefore not limited to the specific details, representative apparatus, and illustrative examples shown and described. Accordingly, departures may be made from such details without departing from the spirit or the scope of Applicants' general inventive concept. The invention is defined in the following claims. In general, the words "first," "second," etc., employed in the claims do not necessarily denote an order.

What is claimed is:

1. In a first system including a plurality of second systems, each second system having a respective identification signal different from the identification signal in the other second systems, a method comprising the steps, performed in each second system, of:

receiving a first signal;

generating a second signal by encrypting using the identification signal, the second signal corresponding to the first signal;

generating a third signal responsive to the second signal, by decrypting using the identification signal; and

conditionally sending the first signal to an output device, depending on the third signal.

2. The method of claim 1 further including receiving a plurality of first signals, wherein the second signal corresponds to the plurality of first signals.

3. The method of claim 1 wherein generating a second signal includes using the identification signal to encrypt a first key, the first key being for decrypting the first signal, and

wherein

conditionally sending the first signal includes decrypting the first signal using the first key.

4. The method of claim 3 wherein decrypting the first signal using the first key includes decrypting a second key using the first key, and decrypting the first signal using the second key.

5. The method of claim 1 wherein generating a third signal includes reading a digital certificate.

6. The method of claim 1 further including receiving a plurality of first signals, wherein the second signal corresponds to the plurality of first signal.

7. The method of claim 1 wherein generating a second signal includes using the identification signal to encrypt a signal derived from a processing history for the first signal.

8. The method of claim 7 wherein the signal derived from a processing history includes a redundancy signal.

9. The method of claim 7 wherein the processing history records a number of times that the first signal may be sent to the output device.

10. A first system comprising:

a plurality of second systems, each second system including

a respective identification signal different from the identification signal in the other second systems;

communication hardware that receives a first signal;

a signal generator that generates a second signal by encrypting using the identification signal, the second signal corresponding to the first signal;

a memory that stores the second signal;

a signal generator that reads from the memory to generate a third signal responsive to the second signal, by decrypting using the identification signal; and

logic that determines whether to send the first signal to an output device, depending on the third signal.

11. The system of claim 10 the communication hardware acts to receive a plurality of first signals,

wherein the second signal corresponds to the plurality of first signals.

12. The system of claim 10 wherein the signal generator that generates a second signal acts to use the identification signal to encrypt a first key, the first key being for decrypting the first signal.

13. The system of claim 12 further including a second key decryptable using the first key, and wherein the first signal is decryptable using the second key.

14. The system of claim 10 further including a digital certificate containing usage information for the first signal.

15. The system of claim 10 the communication hardware acts to receive a plurality of first signals,
wherein the second signal corresponds to the plurality of first signal.

16. The system of claim 10 further wherein the communication hardware receives a plurality of first signals, and
wherein the means for generating a second signal acts to use the identification signal to encrypt a plurality of first keys, each first key being for decrypting a respective one of the first signals.

17. The system of claim 16 wherein the communication hardware receives a plurality of first signals, and
wherein the means for generating a second signal acts to use the identification signal to encrypt a plurality of first keys, each first key being for decrypting a respective one of the first signals,
and each second system further includes a database that stores the encrypted first keys.

18. The system of claim 10 wherein the signal generator that generates a second signal acts to use the identification signal to encrypt a signal derived from a processing history for the first signal.

19. The system of claim 18 wherein the signal derived from a processing history includes a redundancy signal.

20. The system of claim 18 wherein the processing history records a number of times that the first signal may be sent to the output device.

21. A first system comprising a plurality of second systems, each second system including

a respective identification signal different from the identification signal in the other second systems;

means for receiving a first signal;

means for generating a second signal by encrypting using the identification signal, the second signal corresponding to the first signal;

means for generating a third signal responsive to the second signal, by decrypting using the identification signal; and

means for determining whether to send the first signal to an output device, depending on the third signal.

22. The system of claim 21 further wherein the means for receiving acts to receive a plurality of first signals, and wherein the second signal corresponds to the plurality of first signals.

23. The system of claim 21 wherein the means for generating a second signal acts to use the identification signal to encrypt a first key, the first key being for decrypting the first signal, and

wherein

conditionally sending the first signal includes decrypting the first signal using the first key.

24. The system of claim 23 further including a second key decryptable using the first key, and wherein the first signal is decryptable using the second key.

25. The system of claim 21 further wherein the means for receiving acts to receive a plurality of first signals, and

wherein the means for generating a second signal acts to use the identification signal to encrypt a plurality of first keys, each first key being for decrypting a respective one of the first signals.

26. The system of claim 21 wherein the means for receiving acts to receive a plurality of first signals, and

wherein the means for generating a second signal acts to use the identification signal to encrypt a plurality of first keys, each first key being for decrypting a respective one of the first signals,

and each second system further includes a database that stores the encrypted first keys.

27. The system of claim 21 further including a digital certificate containing usage information for the first signal.

28. The system of claim 21 wherein the means for receiving acts to receive a plurality of first signals,

wherein the second signal corresponds to the plurality of first signal.

29. The system of claim 21 further wherein the means for receiving acts to receive a plurality of first signals.

30. The system of claim 21 wherein the means for generating a second signal acts to use the identification signal to encrypt a signal derived from a processing history for the first signal.

31. The system of claim 30 wherein the signal derived from a processing history includes a redundancy signal.

32. The system of claim 30 wherein the processing history records how the first signal may be processed.

33. The system of claim 30 wherein the processing history records a number of times that the first signal may be sent to the output device.

34. In a system including a first signal containing a work, a second signal including a portion of the first signal, and a third signal including an encrypted portion of first signal, a method comprising:

sending a signal to a first output device, by decrypting the third signal;

and the following steps, performed in response to an action by a first consumer,

sending the second and third signals to a second consumer,

and the following steps, performed in response to an action by the second consumer,

conditionally inhibiting the following step, responsive to a fourth signal;

sending a signal to a second output device, by processing the second signal; and

updating the fourth signal, responsive to the previous step.

35. The method of claim 34 wherein processing the second signal includes decrypting the second signal.

36. The method of claim 34 wherein sending the second and third signals includes sending a key for decrypting the second signal.

37. The method of claim 34 wherein sending the second and third signals includes sending a key for decrypting the second signal, and

processing the second signal includes decrypting the second signal using the key.

38. The method of claim 34 wherein sending the second and third signals includes sending a key for decrypting the second signal, without sending a key for decrypting the third signal.

39. The method of claim 34 wherein the second signal includes an introductory portion of the work, and the third signal includes a primary portion of the work.

40. The method of claim 34 wherein updating the fourth signal includes generating a redundancy signal corresponding to the fourth signal.

41. The method of claim 40 further including encrypting the redundancy signal.

42. The method of claim 41 wherein encrypting the redundancy signal includes encrypting the redundancy signal using a key derived from a system identification signal.

43. The method of claim 34 wherein the step of sending the second and third signals sends the second and third signals a first signal path, and the method further includes

sending a key to the second consumer via a second signal path to decrypt the third signal.

44. The method of claim 43 wherein the first signal path includes a portable medium, and the second signal path includes a plurality of computer networks.

45. A system for operating with a first signal containing a work, a second signal including a portion of the first signal, and a third signal including an encrypted portion of first signal, the system comprising:

first circuitry that acts to send a signal to a first output device, by decrypting the third signal; and

second circuitry including

logic to send a signal to a second output device, by processing the second signal,

logic to update a fourth signal in response to the logic to send, and

logic to conditionally inhibiting the logic to send, responsive to a fourth signal.

46. The system of claim 45 further including a first key for decrypting the second signal.

47. The system of claim 46 further including a data structure for associating the first key with the second and third signals.

48. The system of claim 47 further including a second key for decrypting the third signal, wherein the data structure does not associate the second key.

49. The system of claim 45 wherein the second signal includes an introductory portion of the work, and the third signal includes a primary portion of the work.

50. The system of claim 45 wherein the logic to update includes logic to generate a redundancy signal corresponding to the fourth signal.

51. The system of claim 50 wherein the logic to update further includes logic to encrypt the redundancy signal.

52. The system of claim 50 wherein the logic to update further includes logic to encrypt the redundancy signal using a key derived from a system identification signal.

53. A system for operating with a first signal containing a work, a second signal including a portion of the first signal, and a third signal including an encrypted portion of first signal, the system comprising:

means for sending a signal to a first output device, by decrypting the third signal;

means for sending the second and third signals from a first consumer to a second consumer;

means for conditionally inhibiting the following means, responsive to a fourth signal;

means for sending a signal to a second output device, by processing the second signal; and

means for updating the fourth signal, responsive to the previous means.

54. The system of claim 53 further including a first key for decrypting the second signal.

55. The system of claim 54 further including a data structure for associating the first key with the second and third signals.

56. The system of claim 55 further includes a second key for decrypting the third signal, wherein the data structure does not associate the second key.

57. The system of claim 53 wherein the second signal includes an introductory portion of the work, and the third signal includes a primary portion of the work.

58. The system of claim 53 wherein the means for updating includes logic to generate a redundancy signal corresponding to the fourth signal.

59. The system of claim 58 wherein the means for updating further includes logic to encrypt the redundancy signal.

60. The system of claim 58 wherein the means for updating further includes logic to encrypt the redundancy signal using a key derived from a system identification signal.

61. In a system including a plurality of first systems, each first system configured to process a file, a plurality of second systems, each second system configured to process a file, a method comprising:

generating a file having a first part decodable by one of the first systems or second systems, a second part decodable by one of the second systems using a first decryption key, and a third part decodable by one of the second systems without using the first decryption key.

62. The method of claim 61 wherein the third part is decodable by one of the second systems using a second decryption key.

63. A method for a system having a program having a first instruction set that selects a file responsive to a signal from an input device, and a second instruction set that processes a portion of the selected file for sending to an output device, wherein the first instruction set passes control to the second instruction set, responsive to a content of a data structure, the method comprising:

replacing the second instruction set with a third instruction set by setting the content of the data structure to include a direction to the third instruction set, the third instruction set acting to receive the portion of the selected file and decrypt the portion responsive to a decryption key.

64. The method of claim 63 wherein the data structure is a file directory, and setting includes placing an executable file in the directory.

65. The method of claim 63 wherein the third instruction sets sends signal into a signal path toward the output device.

66. In a system including a first signal, a method comprising and the steps, performed for a first consumer, of:

processing the first signal;

sending a signal to a first output device, responsive to the previous step;

and the steps, performed for the second consumer, of

receiving the first signal from the first consumer via a first signal path;

receiving a first key via a second signal path;

processing the first signal using the first key;

sending a signal to a second output device, responsive to the previous step.

67. The method of claim 66 wherein processing the first signal using the first key includes using the first key to decrypt the first signal.

68. The method of claim 66 wherein processing the first signal using the first key includes using the first key to select a second signal, and the method further includes

using the second signal to limit performance of the step of sending a signal to a second output device.

69. The method of claim 68 wherein the second signal includes a digital certificate

70. The method of claim 68 wherein the second signal includes a count of how many times the sending step may be performed

71. The method of claim 66 wherein the system includes a first system under control of the first consumer, the first system having an identification signal, and a second system under control of the second consumer, the second system having an identification

signal different from the identification signal of the first system, wherein the method further includes the step, performed in the first system, of encrypting the first key using the identification signal.

72. The method of claim 66 wherein the system includes a first system under control of the first consumer, the first system having a key for decrypting the first signal, and a second system under control of the second consumer, wherein the method further includes the step, performed in the first system, of

sending the first signal to the second consumer without sending the key for decrypting the first signal.

73. The method of claim 66 wherein the first signal path includes a portable medium, and the second signal path includes a plurality of computer networks.

74. A system comprising:

a first system including

a first output device;

a processor that processes the first signal to generate a first processed signal;

a sender that sends the first processed signal to the first output device;

a second system including

a second output device;

communication hardware that acts to receive the first signal via a first signal path, and receive a first key via a second signal path;

a processor that processes the first signal, using the first key, to generate a second processed signal;

a sender that sends the second processed signal to the second output device,

wherein the first system includes communication hardware that sends the first signal to the second system.

75. The system of claim 74 wherein the processor in the second system acts to use the first key to decrypt the first signal.

76. The system of claim 74 wherein the processor in the second system acts to use the first key to select a second signal, and to use the second signal to limit performance of the sender in the second system.

77. The system of claim 76 wherein the second signal includes a digital certificate

78. The system of claim 76 wherein the second signal includes a count of how many times the sender may operate.

79. The system of claim 74 wherein the first system has an identification signal, and the second system has an identification signal different from the identification signal of the first system, wherein the processor in the first system acts encrypt the first key using the identification signal.

80. The system of claim 74 wherein the first signal path includes a portable medium, and the second signal path includes a plurality of computer networks.

81. A system comprising:

first means for processing a first signal;

means for sending a signal to a first output device, responsive to the previous means;

means for receiving the first signal from the first means for processing via a first signal path;

means for receiving a first key via a second signal path;

second means for processing the received first signal using the first key; and

means for sending a signal to a second output device, responsive to the previous means.

82. The system of claim 81 wherein the second means for processing acts to use the first key to decrypt the first signal.

83. The system of claim 81 wherein the second means for processing acts to use the first key to select a second signal, and to use the second signal to limit performance of the means for sending a signal to a second output device.

84. The system of claim 83 wherein the second signal includes a digital certificate

85. The system of claim 83 wherein the second signal includes a count of how many times the means for sending, to the second output device, may operate.

86. The system of claim 81 wherein the first means for processing has an identification signal, and the second means for processing has an identification signal different from the identification signal of the first system, wherein the processor in the first system acts encrypt the first key using the identification signal.

87. The system of claim 81 wherein the first signal path includes a portable medium, and the second signal path includes a plurality of computer networks.

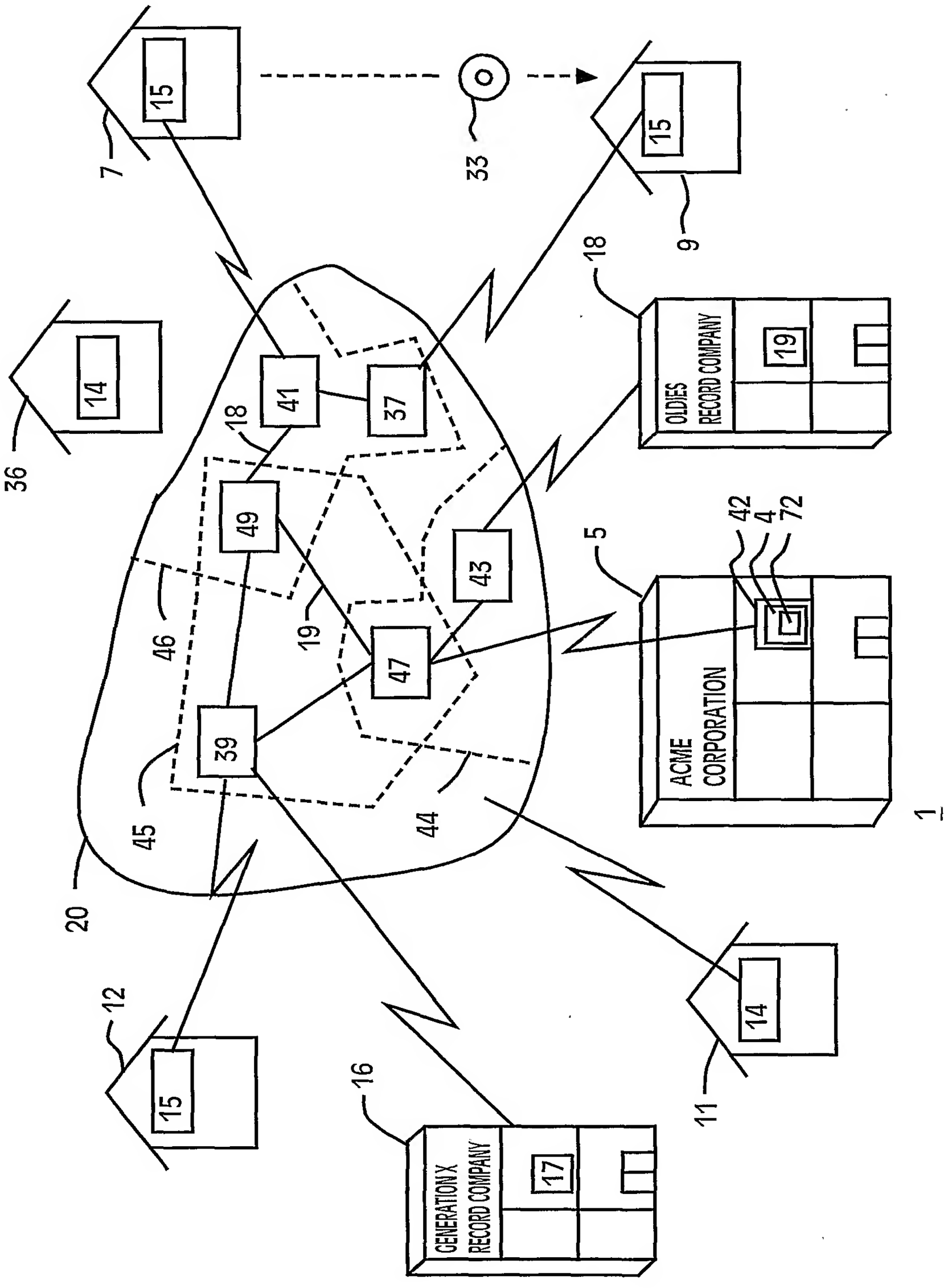

15
7
33
15
9
18
OLDIES RECORD COMPANY
19
14
36
41
37
18
49
43
46
19
47
39
45
44
5
42
4
72
ACME CORPORATION
1
20
12
15
16
GENERATION X RECORD COMPANY
17
14
11

Fig. 1

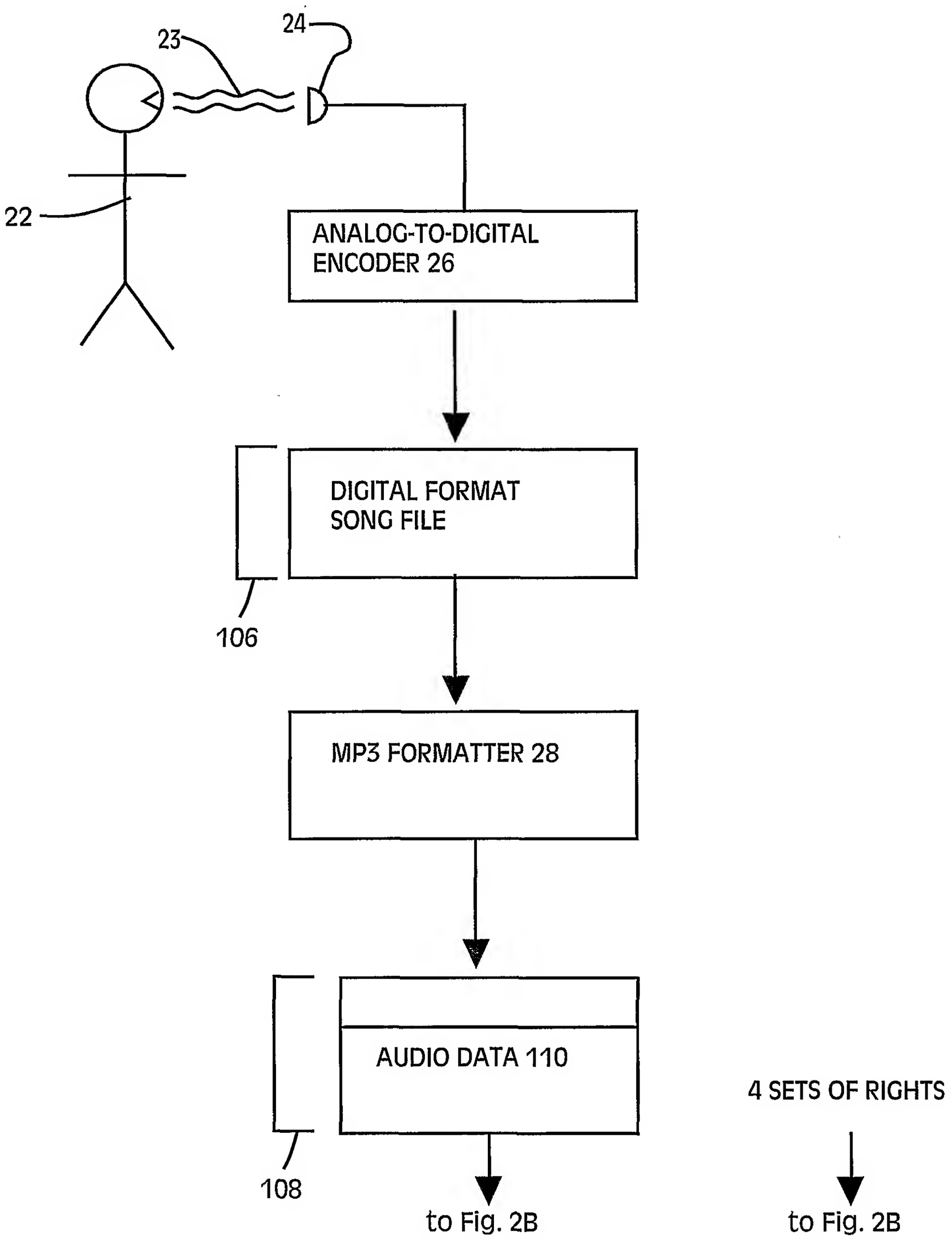

23
24
22
ANALOG-TO-DIGITAL ENCODER 26
DIGITAL FORMAT SONG FILE
106
MP3 FORMATTER 28
AUDIO DATA 110
108
to Fig. 2B
4 SETS OF RIGHTS
to Fig. 2B

FIG. 2A

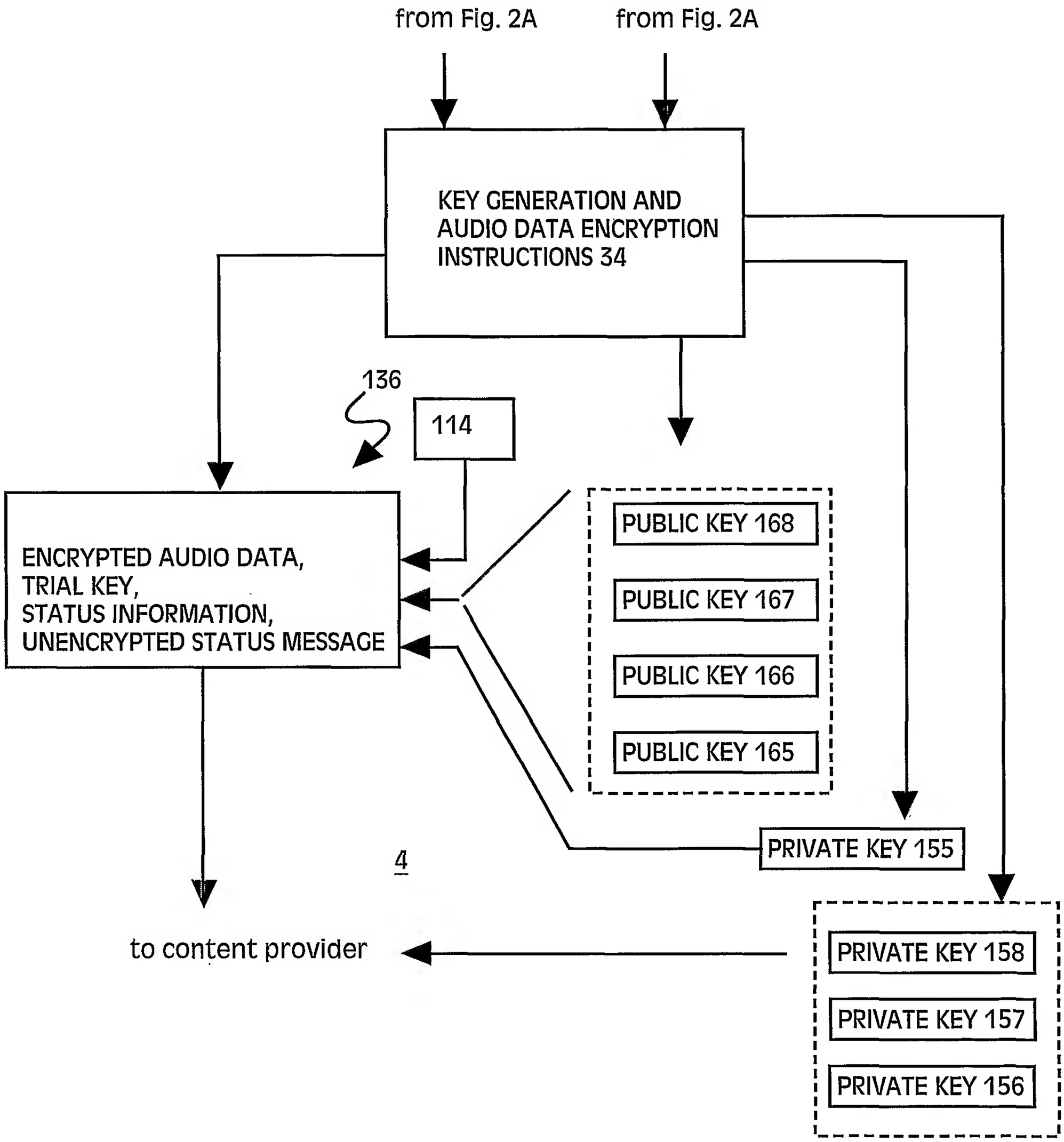

from Fig. 2A
from Fig. 2A
KEY GENERATION AND AUDIO DATA ENCRYPTION INSTRUCTIONS 34
136
114
ENCRYPTED AUDIO DATA,
TRIAL KEY,
STATUS INFORMATION,
UNENCRYPTED STATUS MESSAGE
PUBLIC KEY 168
PUBLIC KEY 167
PUBLIC KEY 166
PUBLIC KEY 165
PRIVATE KEY 155
4
to content provider
PRIVATE KEY 158
PRIVATE KEY 157
PRIVATE KEY 156

FIG. 2B

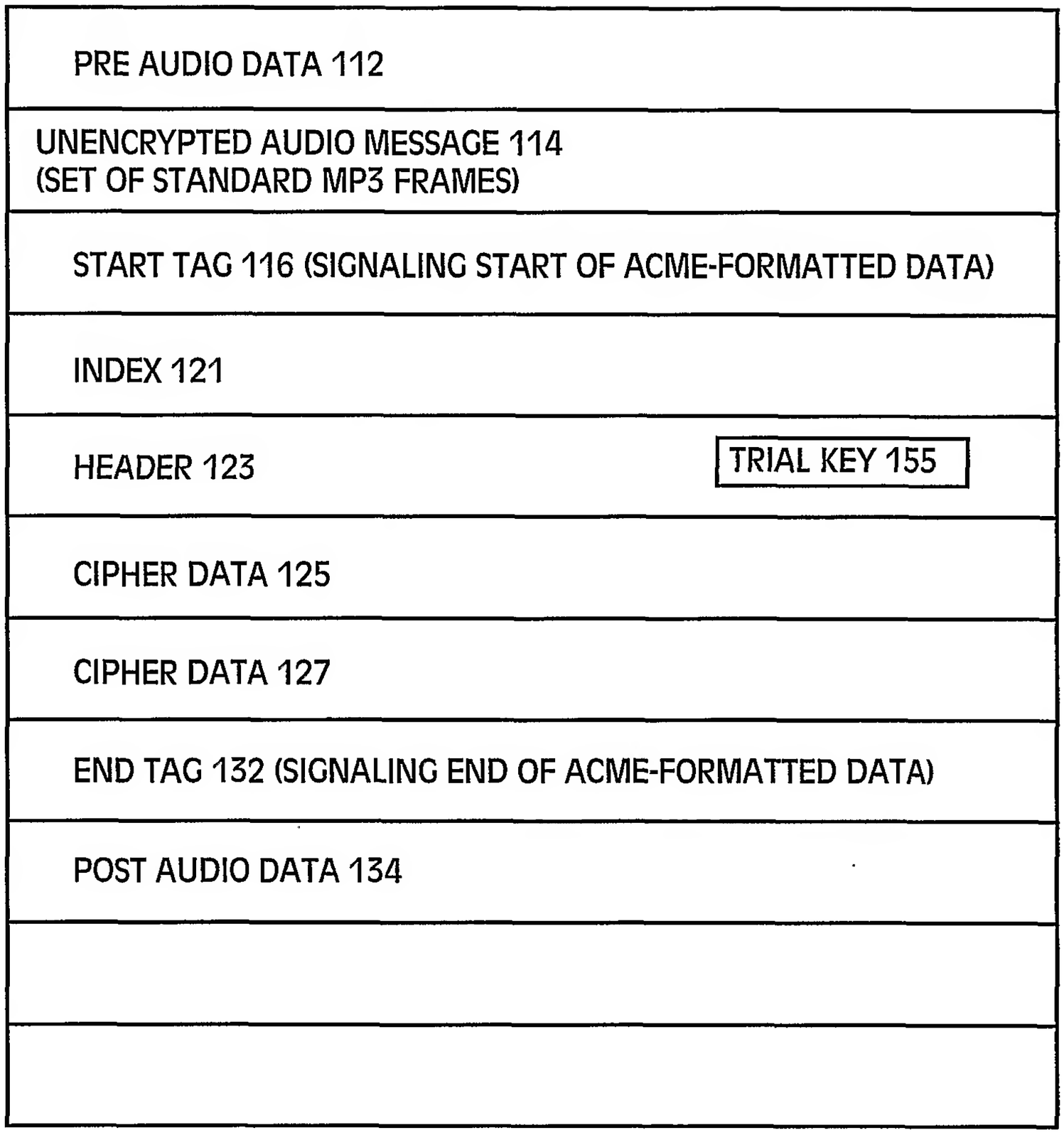
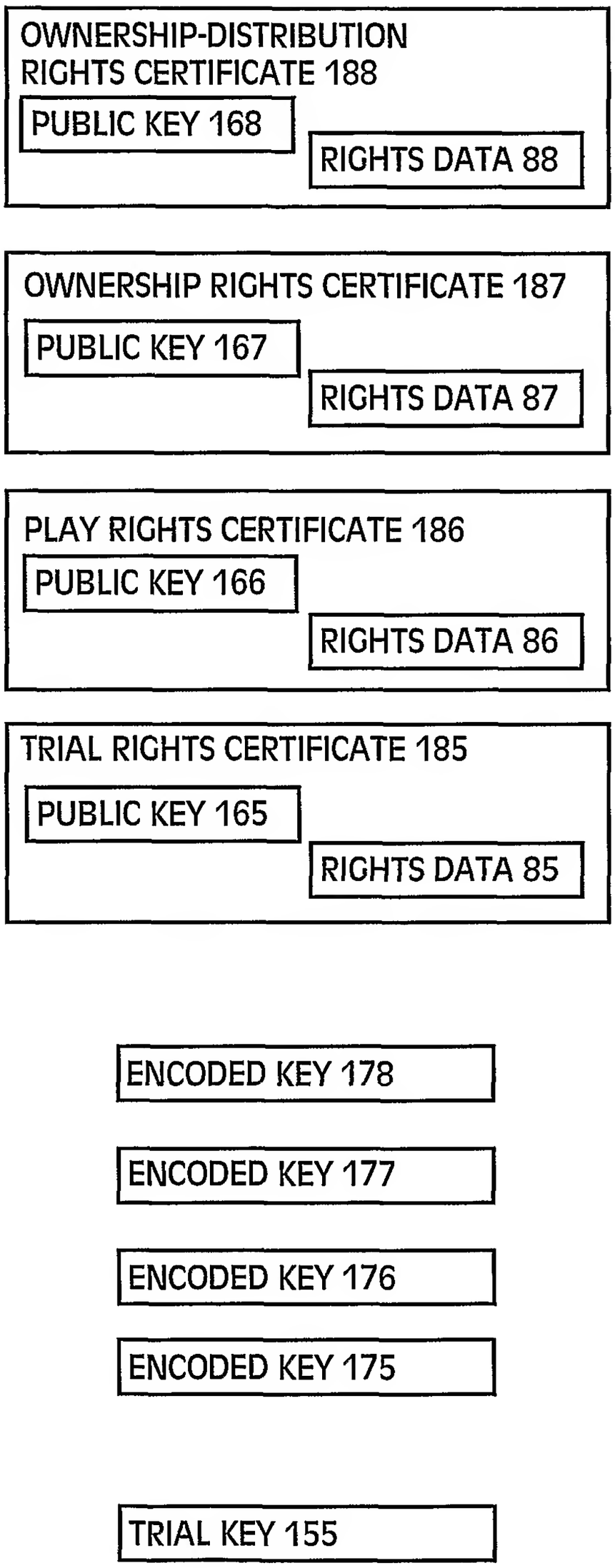

PRE AUDIO DATA 112
UNENCRYPTED AUDIO MESSAGE 114
(SET OF STANDARD MP3 FRAMES)
START TAG 116 (SIGNALING START OF ACME-FORMATTED DATA)
INDEX 121
HEADER 123
TRIAL KEY 155
CIPHER DATA 125
CIPHER DATA 127
END TAG 132 (SIGNALING END OF ACME-FORMATTED DATA)
POST AUDIO DATA 134
136

FIG. 3


OWNERSHIP-DISTRIBUTION RIGHTS CERTIFICATE 188
PUBLIC KEY 168
RIGHTS DATA 88
OWNERSHIP RIGHTS CERTIFICATE 187
PUBLIC KEY 167
RIGHTS DATA 87
PLAY RIGHTS CERTIFICATE 186
PUBLIC KEY 166
RIGHTS DATA 86
TRIAL RIGHTS CERTIFICATE 185
PUBLIC KEY 165
RIGHTS DATA 85
ENCODED KEY 178
ENCODED KEY 177
ENCODED KEY 176
ENCODED KEY 175
TRIAL KEY 155

123

FIG. 4

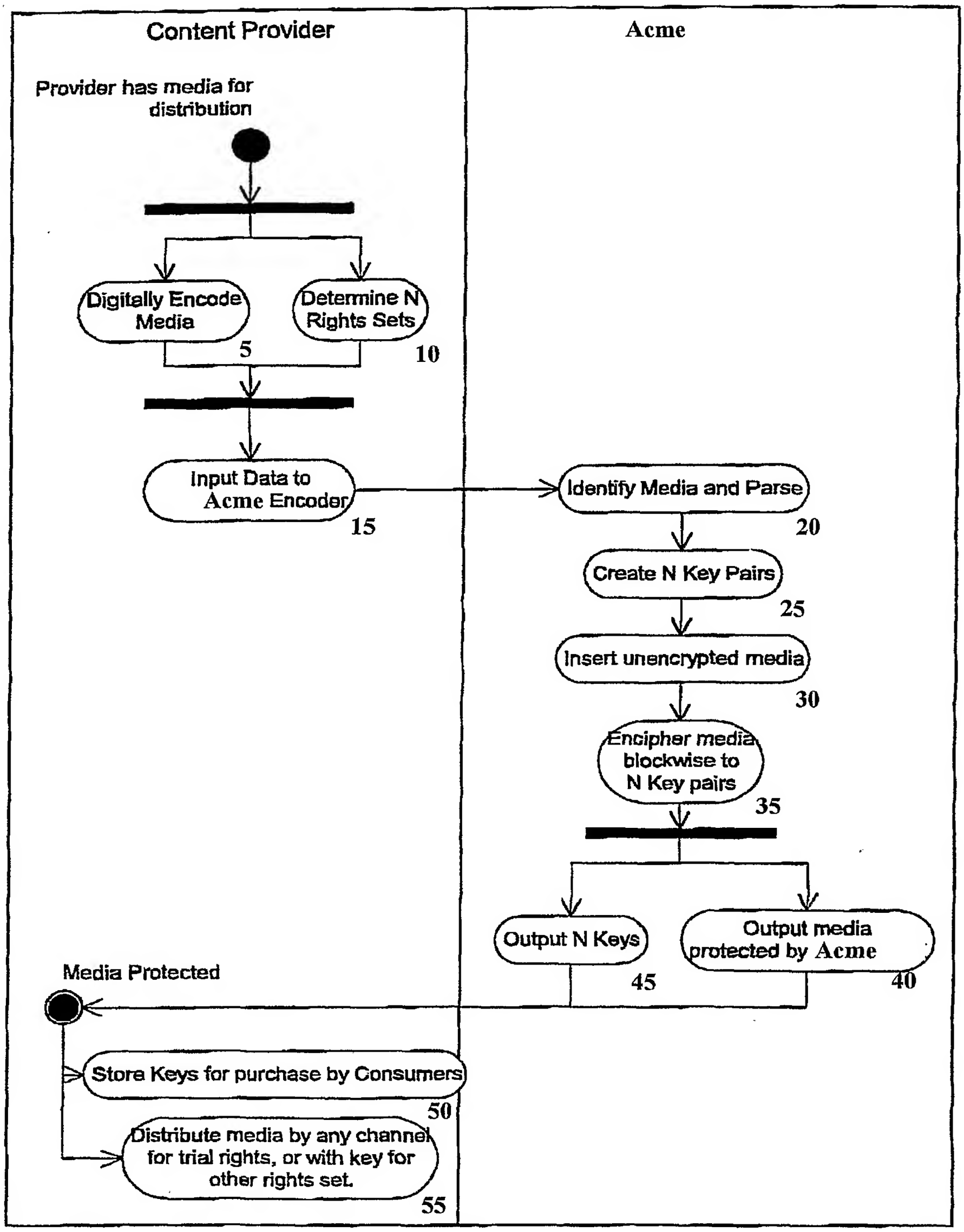

Content Provider
Acme
Provider has media for distribution
Digitally Encode Media
Determine N Rights Sets
5
10
Input Data to Acme Encoder
15
Identify Media and Parse
20
Create N Key Pairs
25
Insert unencrypted media
30
Encipher media blockwise to N Key pairs
35
Output N Keys
45
Output media protected by Acme
40
Media Protected
Store Keys for purchase by Consumers
50
Distribute media by any channel for trial rights, or with key for other rights set.
55

Fig. 5

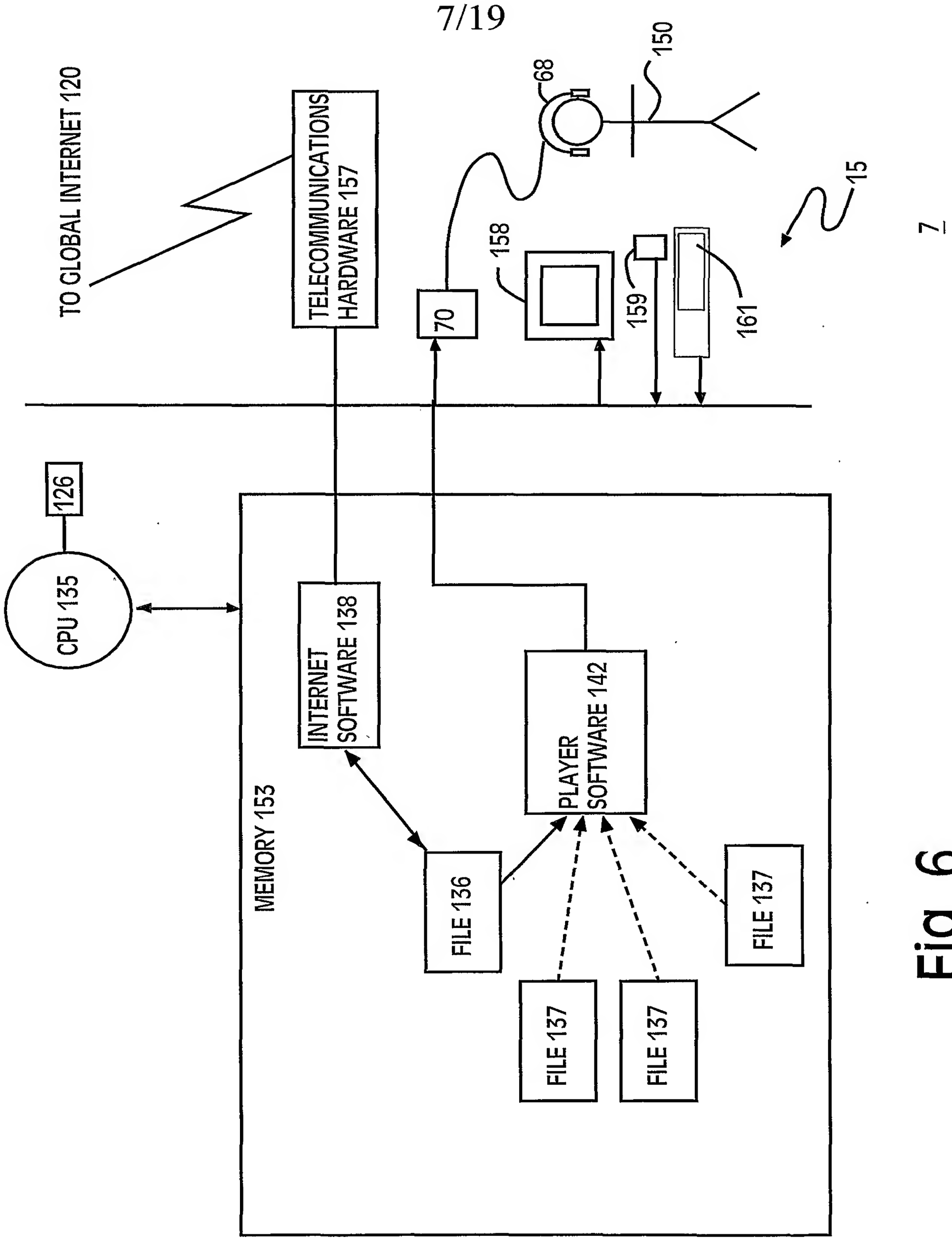

TO GLOBAL INTERNET 120
TELECOMMUNICATIONS HARDWARE 157
68
150
15
7
158
70
159
161
126
CPU 135
MEMORY 153
INTERNET SOFTWARE 138
PLAYER SOFTWARE 142
FILE 136
FILE 137
FILE 137
FILE 137

Fig. 6

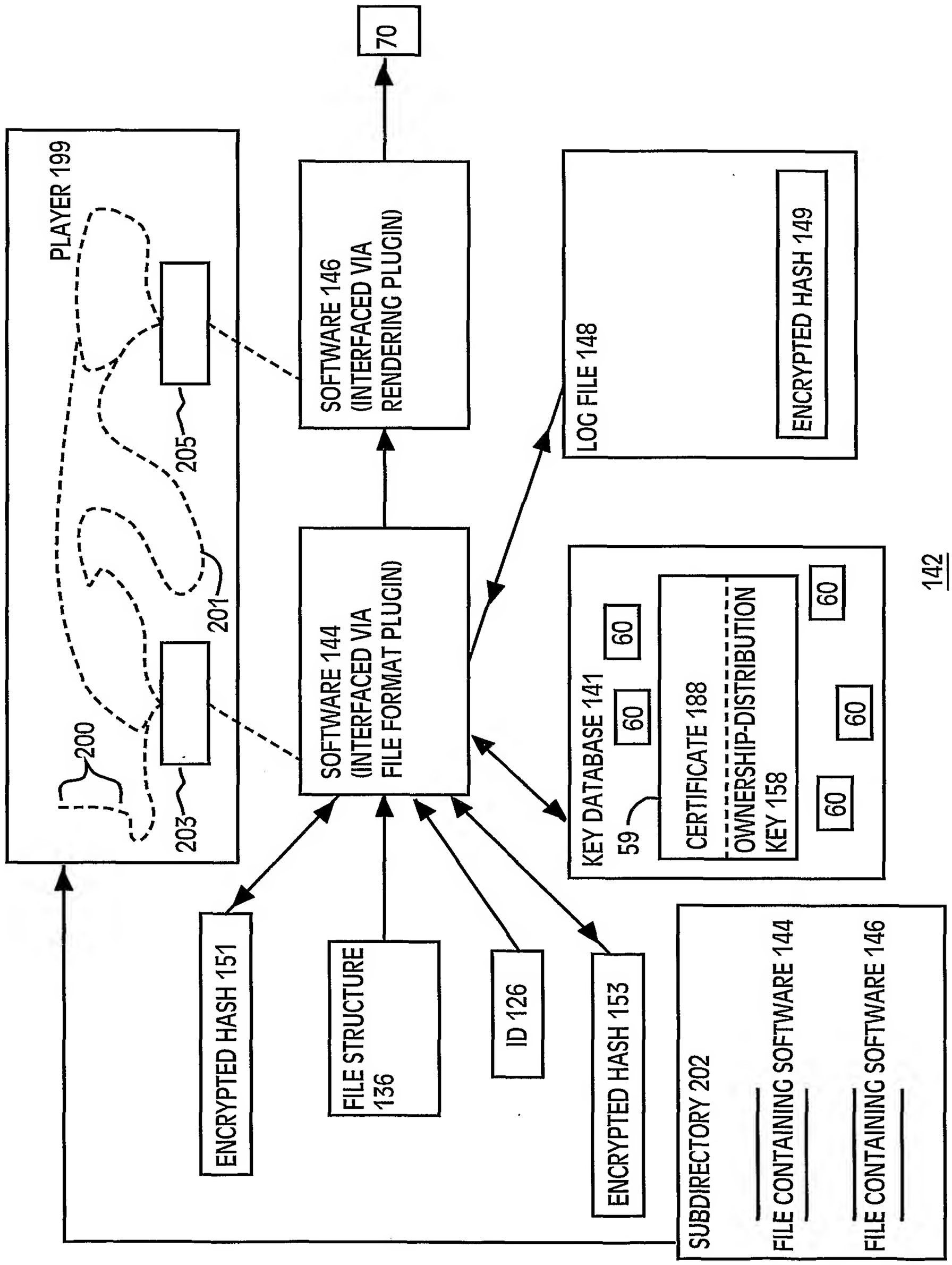

70
PLAYER 199
200
201
203
205
SOFTWARE 146 (INTERFACED VIA RENDERING PLUGIN)
SOFTWARE 144 (INTERFACED VIA FILE FORMAT PLUGIN)
LOG FILE 148
ENCRYPTED HASH 149
KEY DATABASE 141
59
60
CERTIFICATE 188
OWNERSHIP-DISTRIBUTION KEY 158
142
ENCRYPTED HASH 151
FILE STRUCTURE 136
ID 126
ENCRYPTED HASH 153
SUBDIRECTORY 202
FILE CONTAINING SOFTWARE 144
FILE CONTAINING SOFTWARE 146

Fig. 7

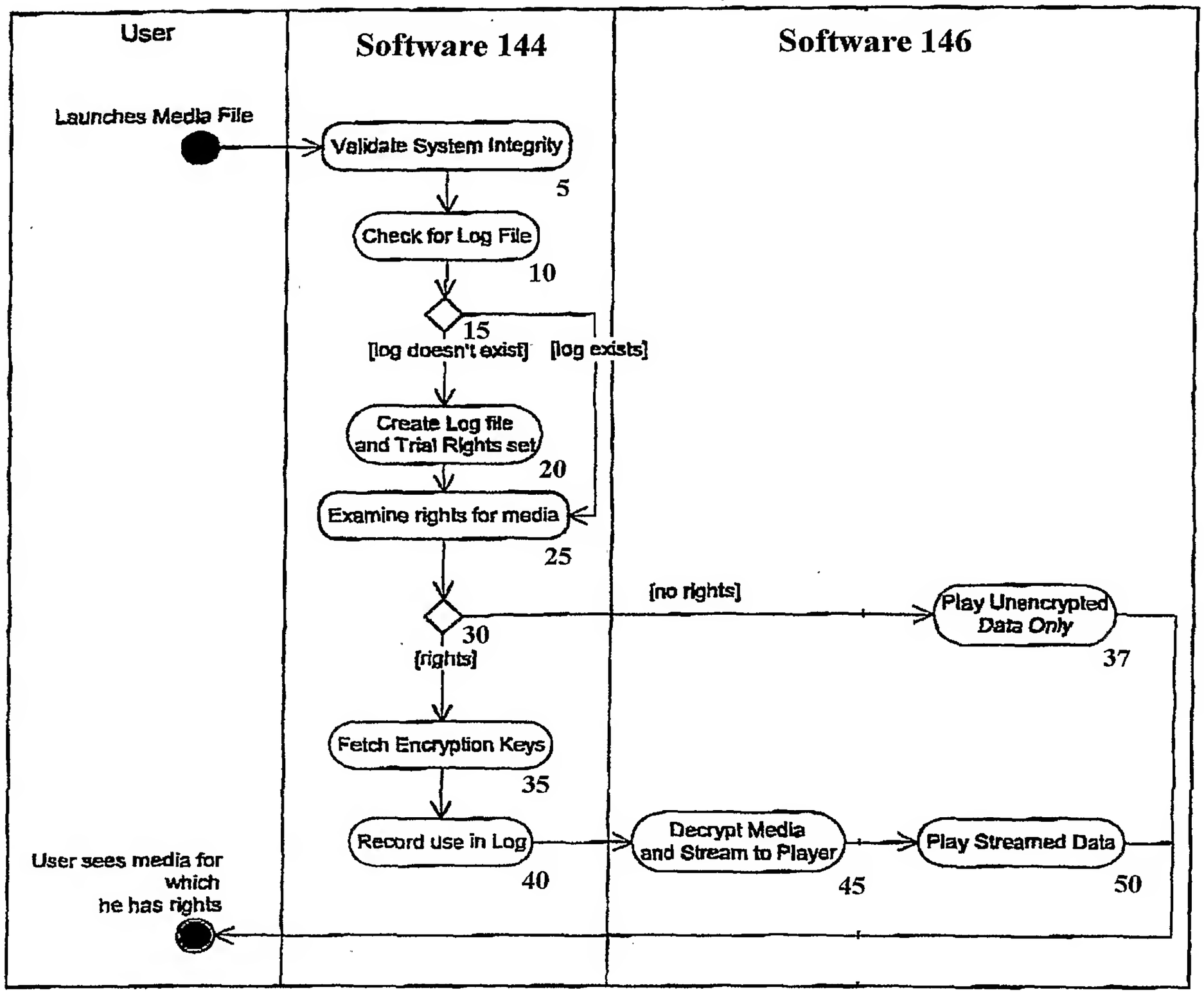

User
Software 144
Software 146
Launches Media File
Validate System Integrity
5
Check for Log File
10
15
[log doesn't exist]
[log exists]
Create Log file and Trial Rights set
20
Examine rights for media
25
30
[rights]
[no rights]
Play Unencrypted Data Only
37
Fetch Encryption Keys
35
Record use in Log
40
Decrypt Media and Stream to Player
45
Play Streamed Data
50
User sees media for which he has rights

Fig. 8

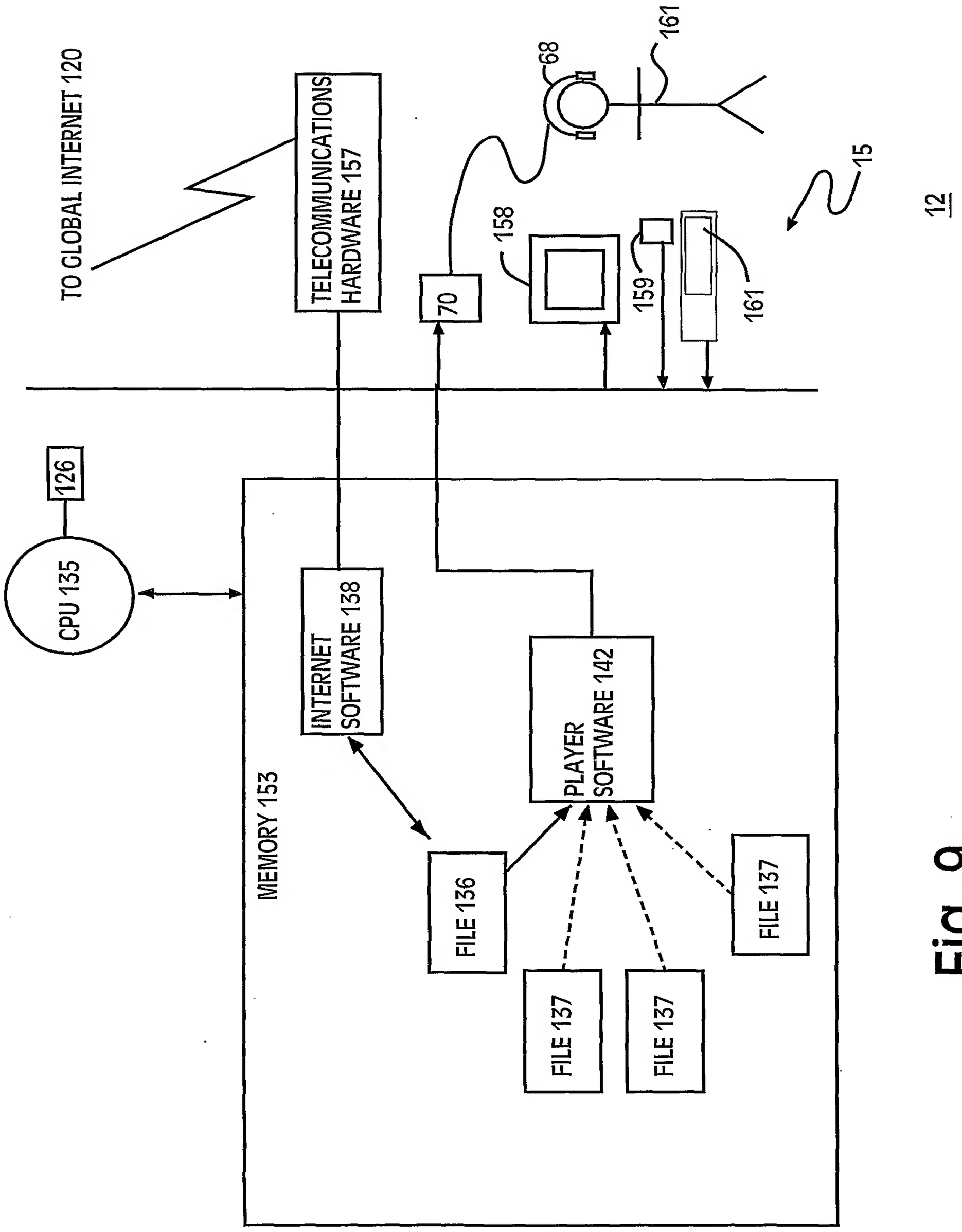

TO GLOBAL INTERNET 120
TELECOMMUNICATIONS HARDWARE 157
68
161
15
12
158
70
159
161
126
CPU 135
MEMORY 153
INTERNET SOFTWARE 138
PLAYER SOFTWARE 142
FILE 136
FILE 137
FILE 137
FILE 137

Fig. 9

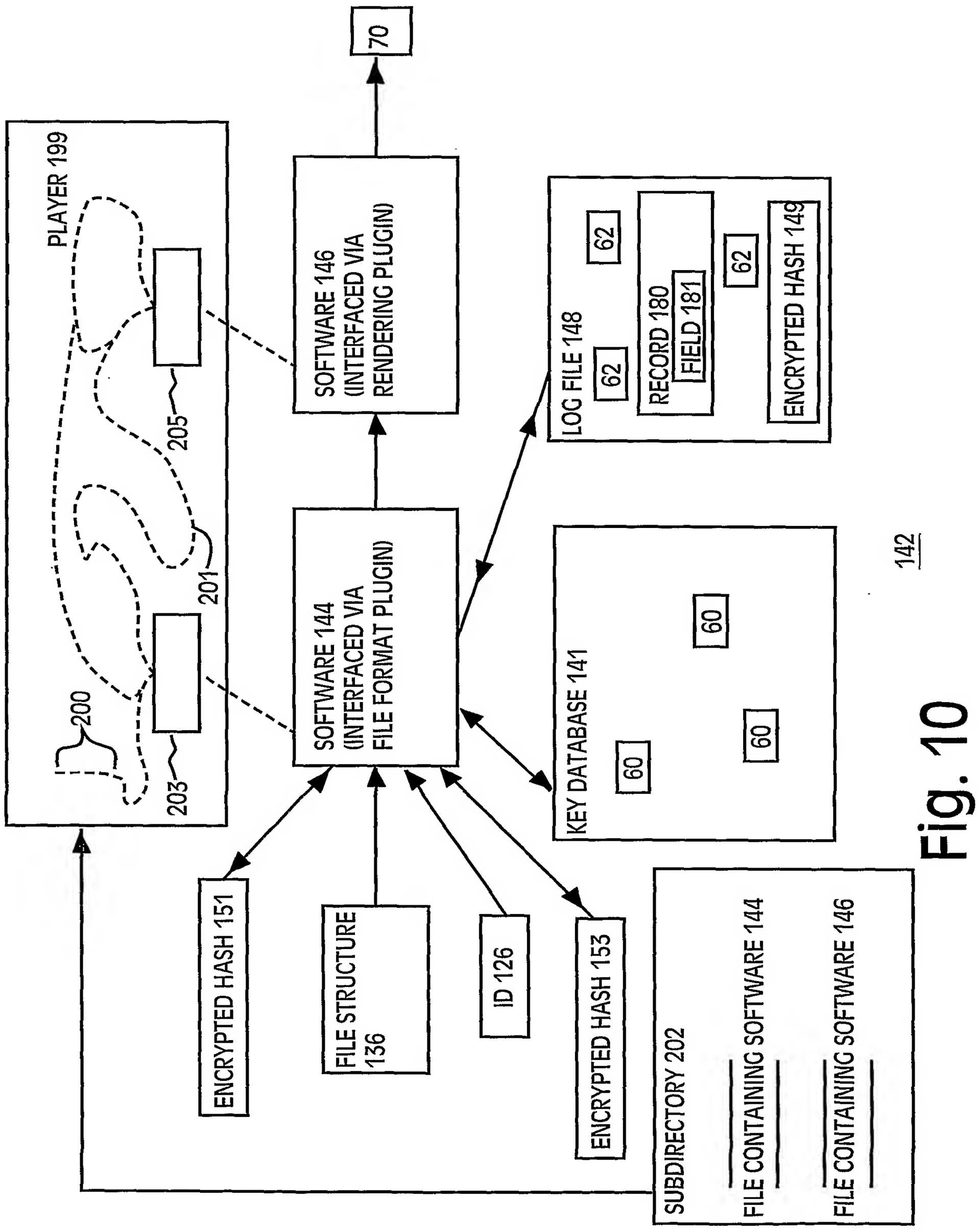

70
PLAYER 199
200
201
203
205
SOFTWARE 146 (INTERFACED VIA RENDERING PLUGIN)
SOFTWARE 144 (INTERFACED VIA FILE FORMAT PLUGIN)
LOG FILE 148
62
RECORD 180
FIELD 181
ENCRYPTED HASH 149
KEY DATABASE 141
60
142
ENCRYPTED HASH 151
FILE STRUCTURE 136
ID 126
ENCRYPTED HASH 153
SUBDIRECTORY 202
FILE CONTAINING SOFTWARE 144
FILE CONTAINING SOFTWARE 146

Fig. 10

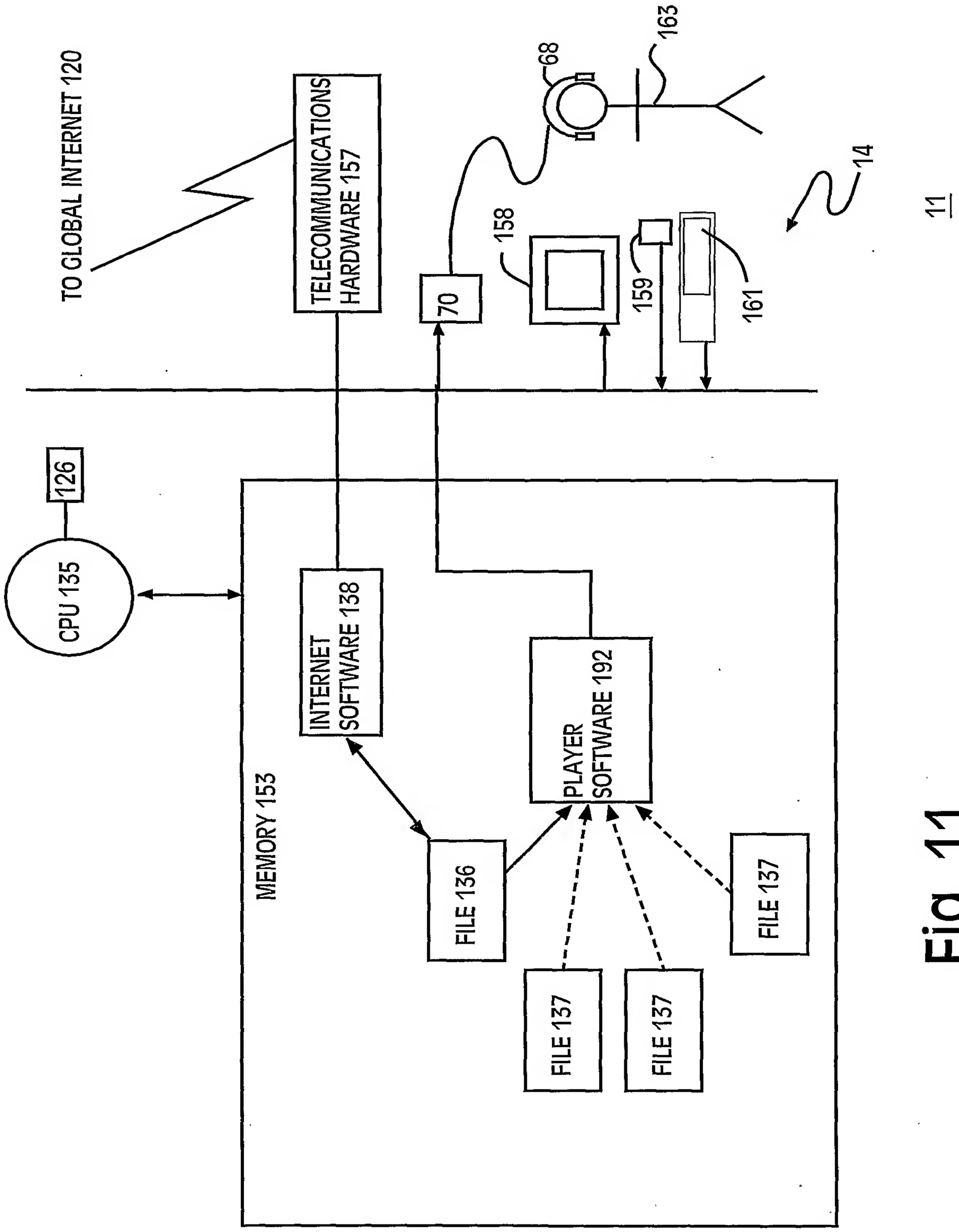

TO GLOBAL INTERNET 120
TELECOMMUNICATIONS HARDWARE 157
68
163
14
11
158
159
161
70
126
CPU 135
MEMORY 153
INTERNET SOFTWARE 138
PLAYER SOFTWARE 192
FILE 136
FILE 137
FILE 137
FILE 137

Fig. 11

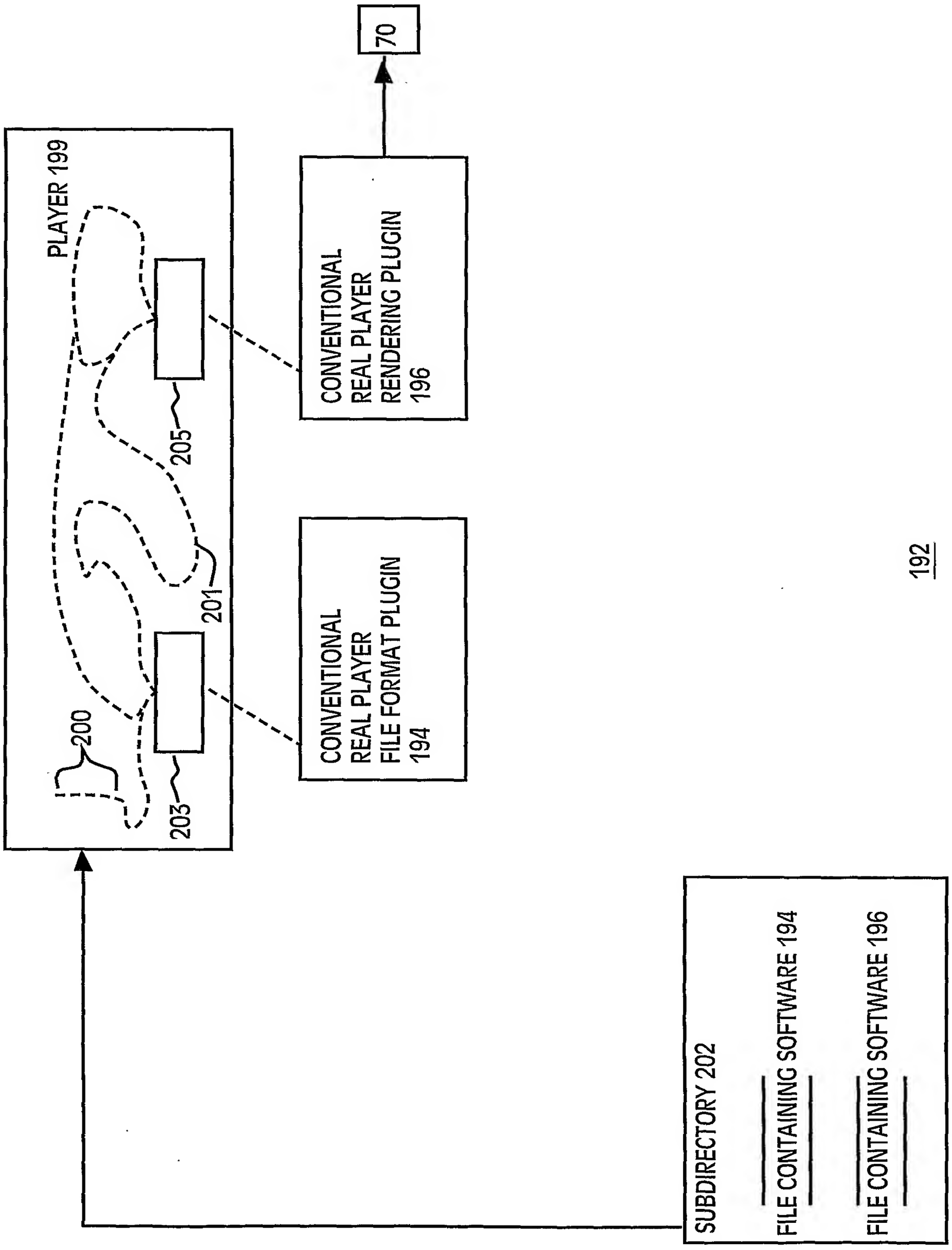

192
SUBDIRECTORY 202
FILE CONTAINING SOFTWARE 194
FILE CONTAINING SOFTWARE 196
PLAYER 199
200
201
203
205
CONVENTIONAL REAL PLAYER FILE FORMAT PLUGIN 194
CONVENTIONAL REAL PLAYER RENDERING PLUGIN 196
70

Fig. 12

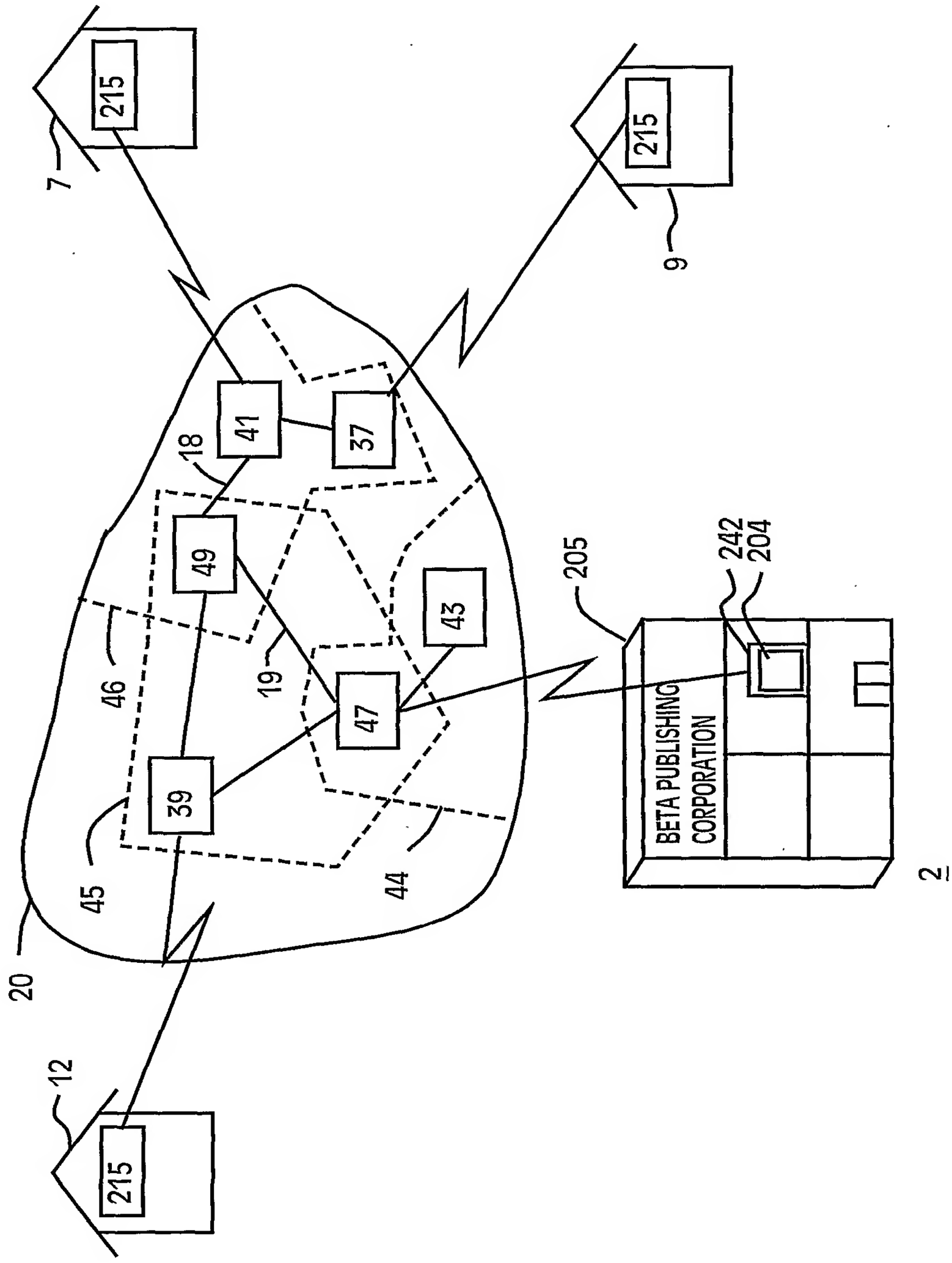

215
7
215
9
41
37
18
49
43
46
19
47
39
45
44
20
205
242
204
BETA PUBLISHING
CORPORATION
2
12
215

Fig. 13

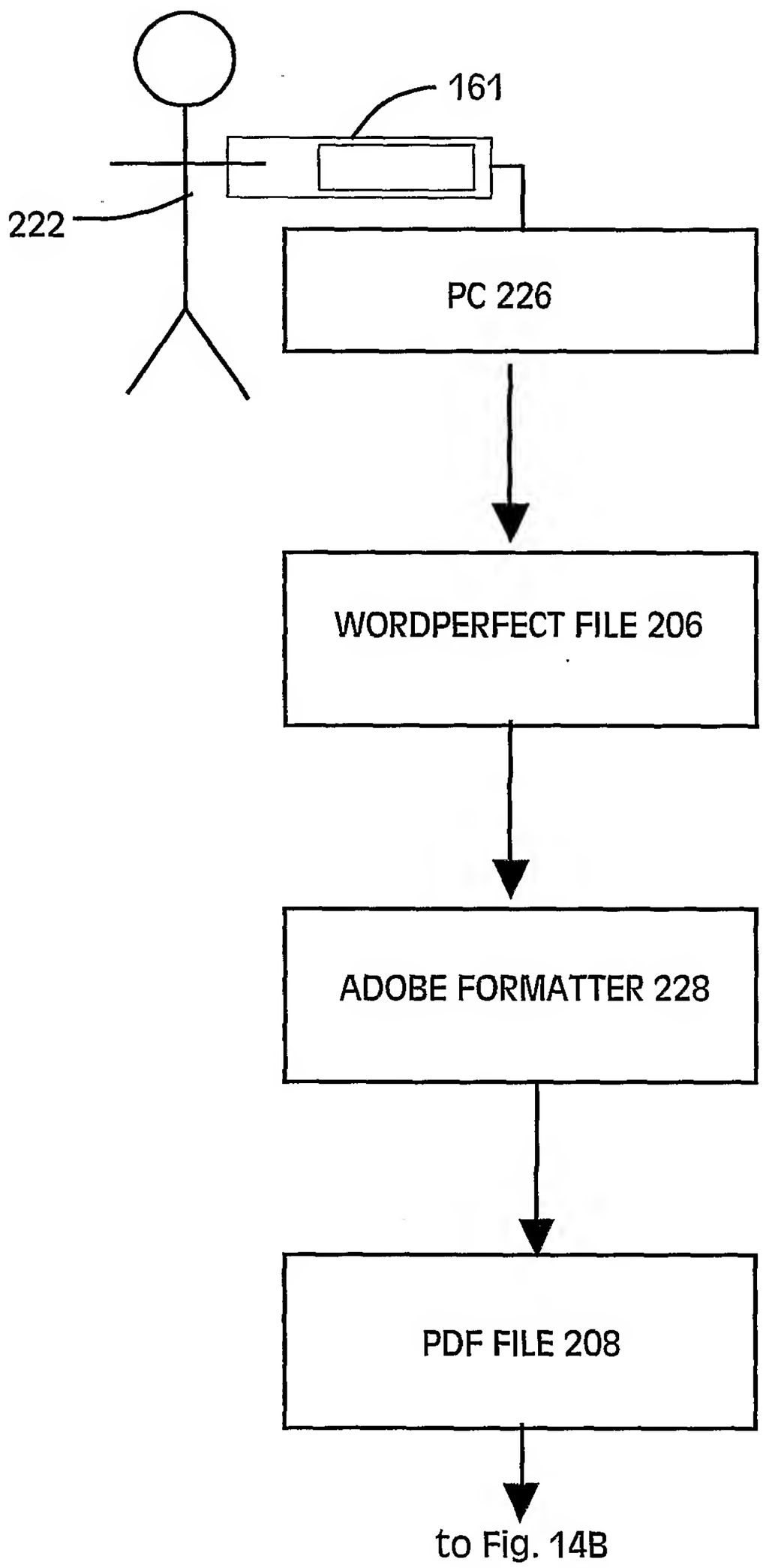

161
222
PC 226
WORDPERFECT FILE 206
ADOBE FORMATTER 228
PDF FILE 208
to Fig. 14B

FIG. 14A

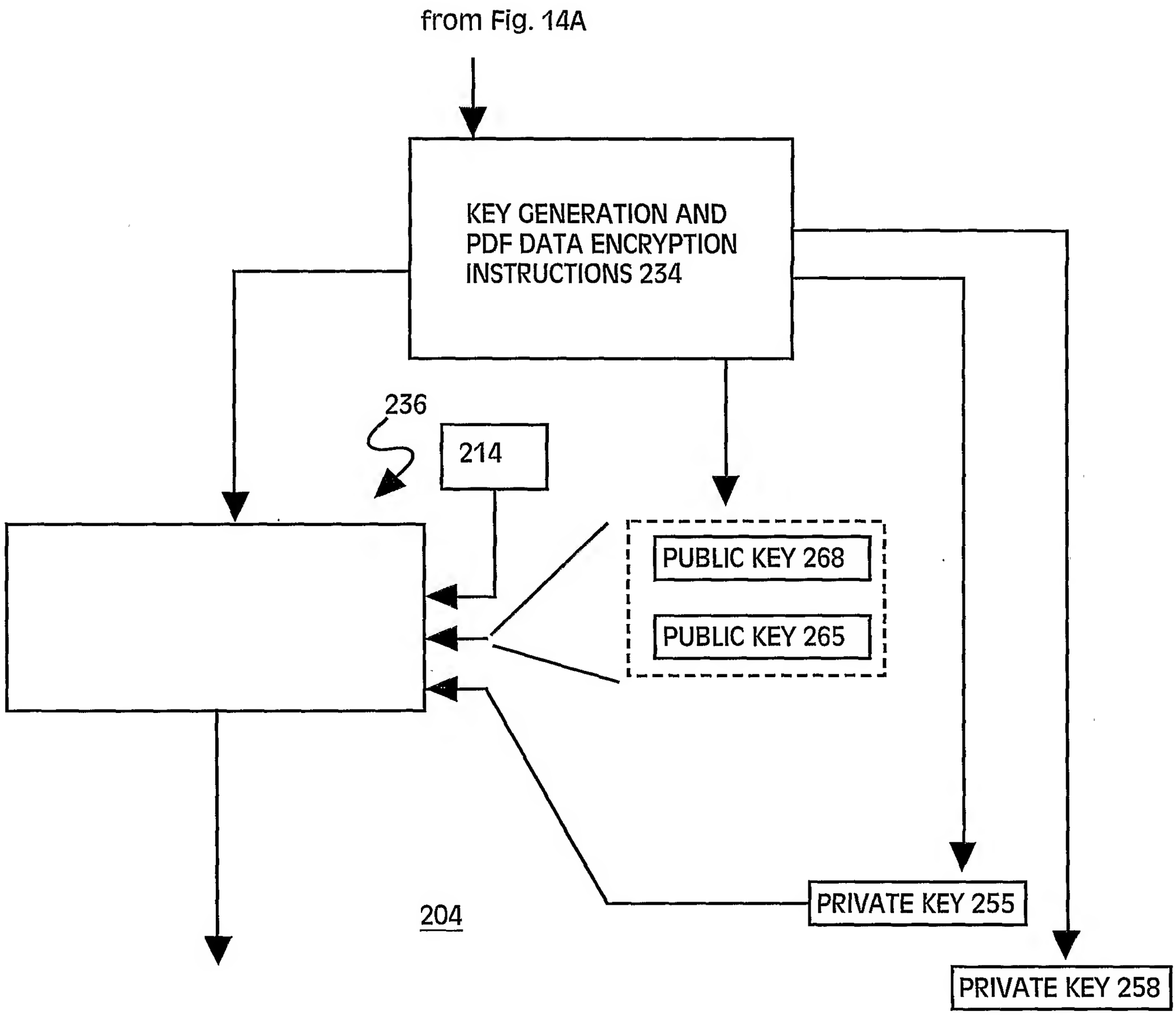

from Fig. 14A
KEY GENERATION AND PDF DATA ENCRYPTION INSTRUCTIONS 234
236
214
PUBLIC KEY 268
PUBLIC KEY 265
PRIVATE KEY 255
PRIVATE KEY 258
204

FIG. 14B

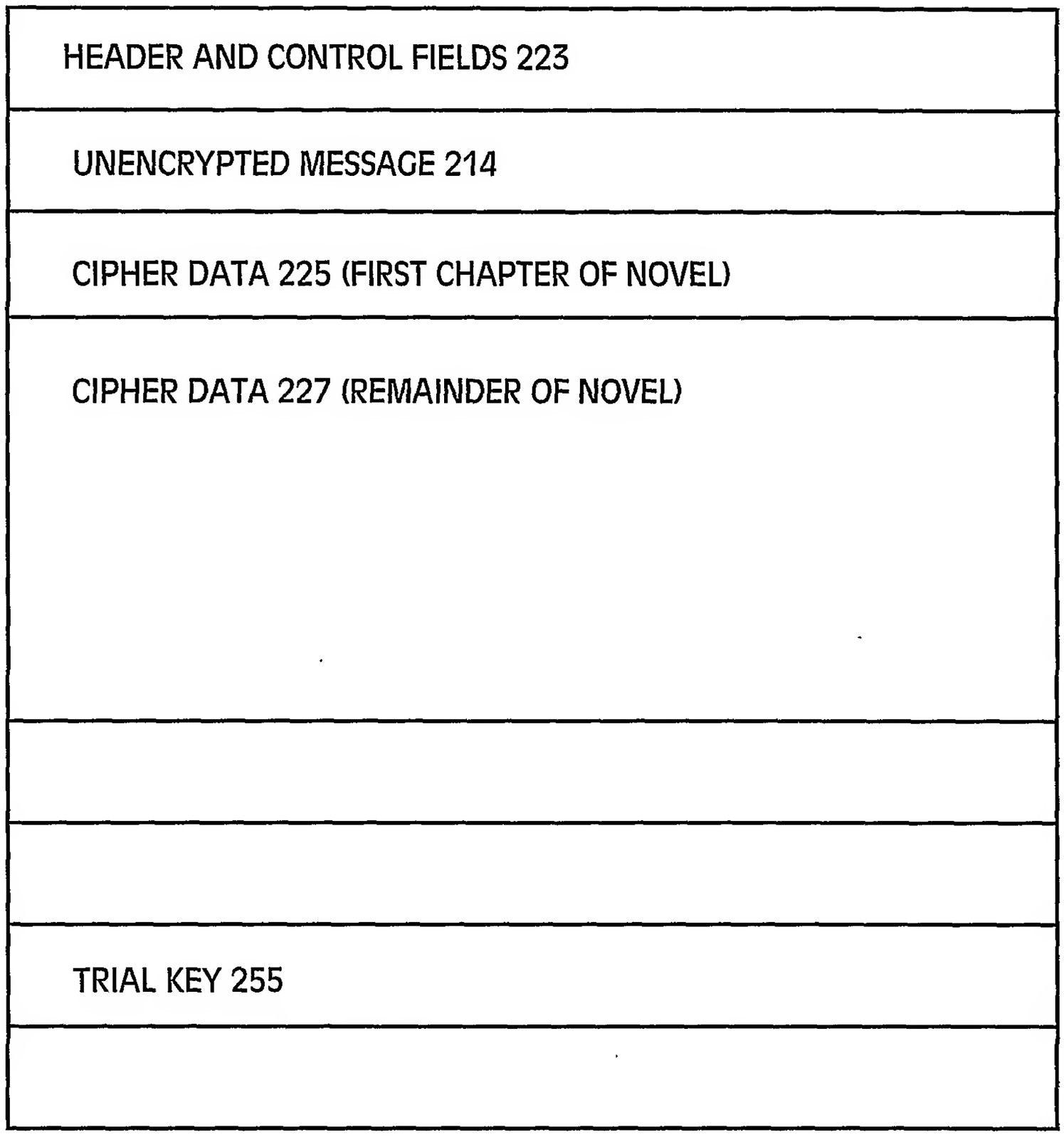

HEADER AND CONTROL FIELDS 223
UNENCRYPTED MESSAGE 214
CIPHER DATA 225 (FIRST CHAPTER OF NOVEL)
CIPHER DATA 227 (REMAINDER OF NOVEL)
TRIAL KEY 255
236

FIG. 15

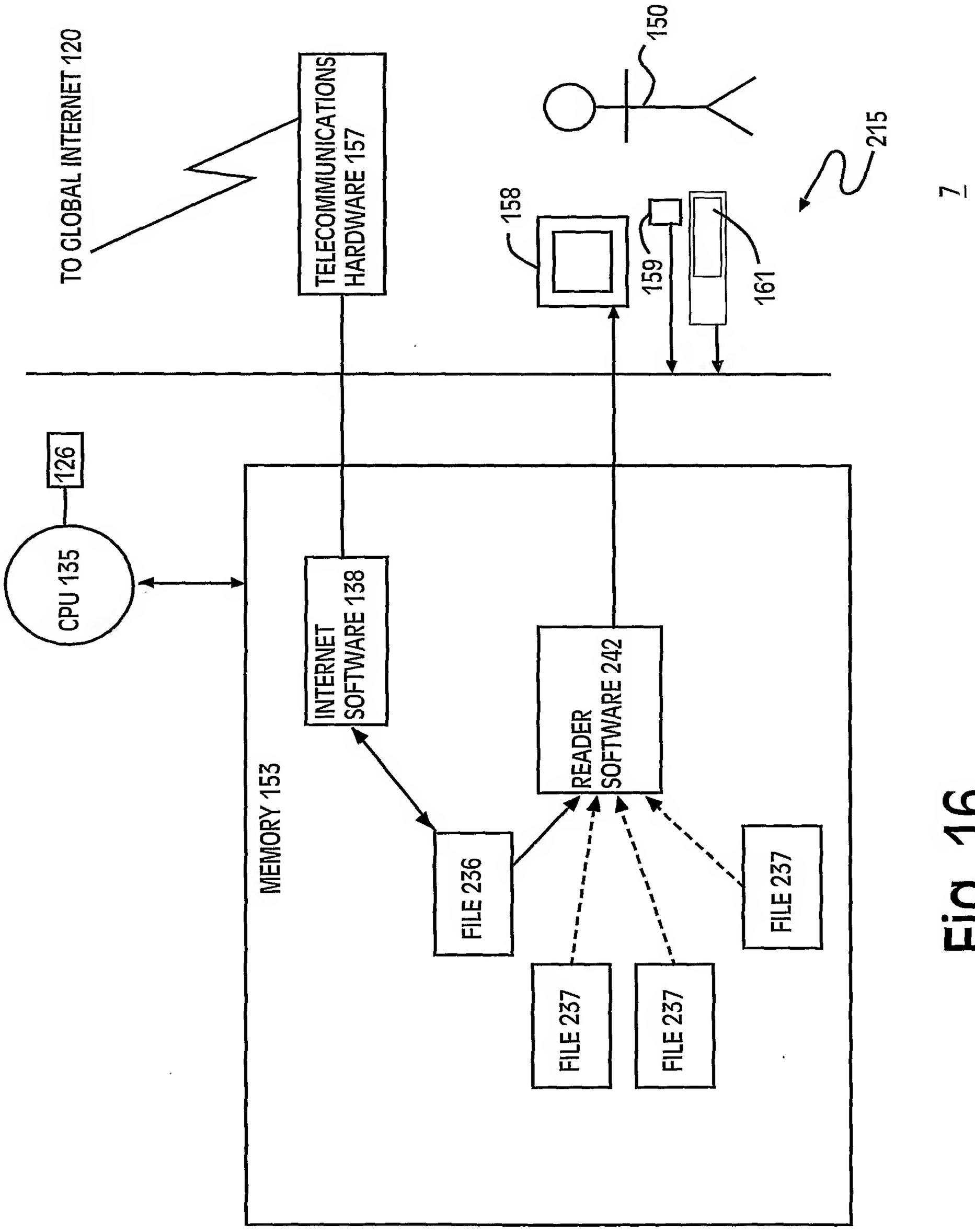

TO GLOBAL INTERNET 120
TELECOMMUNICATIONS HARDWARE 157
150
215
158
159
161
7
126
CPU 135
MEMORY 153
INTERNET SOFTWARE 138
READER SOFTWARE 242
FILE 236
FILE 237
FILE 237
FILE 237

Fig. 16

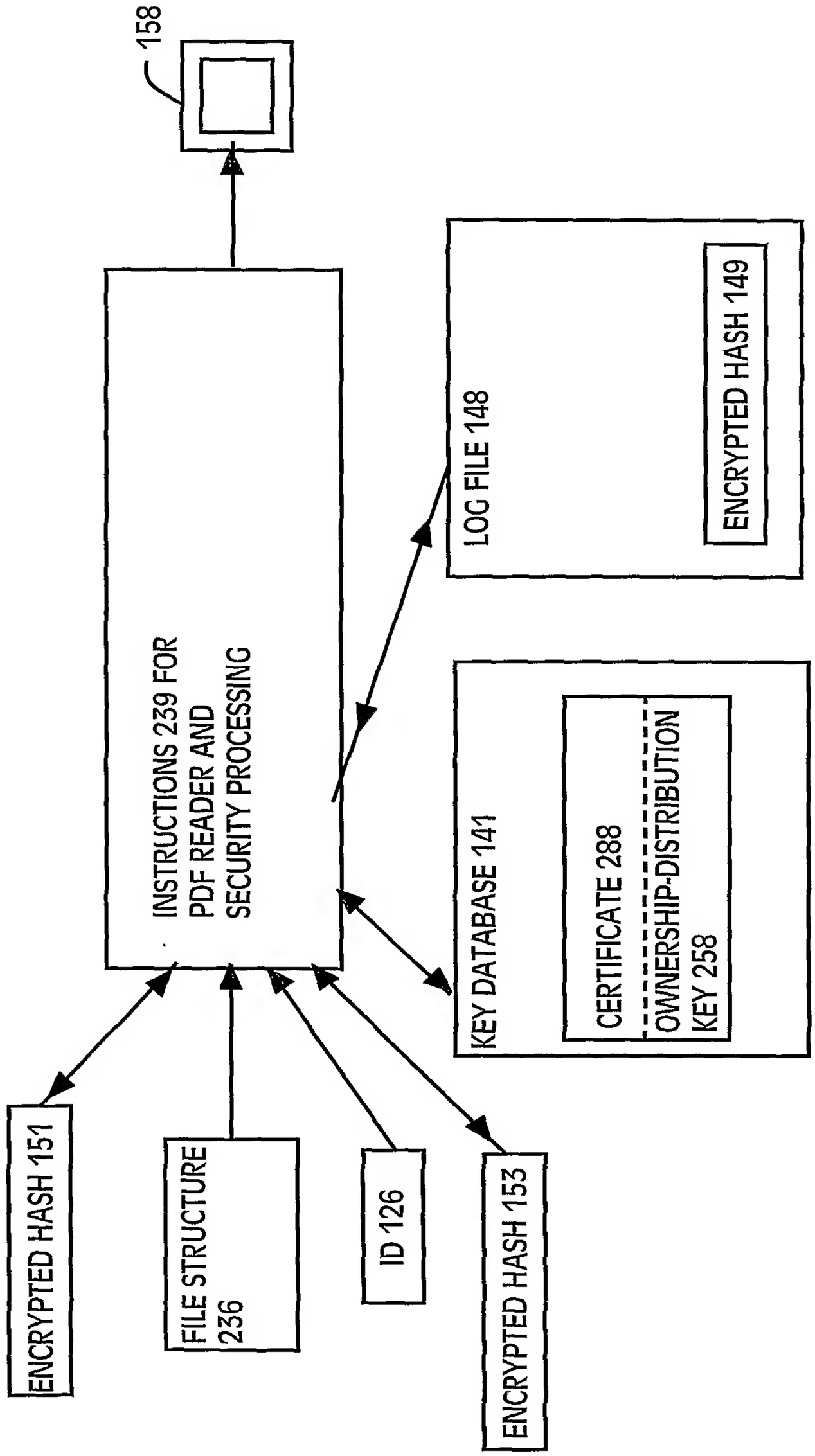

158
INSTRUCTIONS 239 FOR PDF READER AND SECURITY PROCESSING
LOG FILE 148
ENCRYPTED HASH 149
KEY DATABASE 141
CERTIFICATE 288
OWNERSHIP-DISTRIBUTION KEY 258
ENCRYPTED HASH 151
FILE STRUCTURE 236
ID 126
ENCRYPTED HASH 153
242

Fig. 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/28348

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04N 7/167; H04K 1/00
US CL : 380/201, 202, 203; 705/57, 58, 59
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/201, 202, 203; 705/57, 58, 59

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Menezes, *Handbook of Applied Cryptography*, CRC Press

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Dialog, STN, West, Internet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,915,018 A (AUCSMITH) 22 June 1999 Figure 2, 4 (a) (b) , *Columns* 3-7	1-87
Y	US 5,513,260 A (RYAN) 30 April 1996, Columns 4-8	1-87
Y	US 4,172,213 A (BARNES et. al.) 23 October 1979, Columns 4-7, 9	1-87
Y	MENEZES et. al. Handbook of Applied Cryptography, Chapter 10	1-87

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 16 DECEMBER 2001	Date of mailing of the international search report 15 JAN 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 746-7239	Authorized officer GAIL HAYES Telephone No. (703) 308-4562

Form PCT/ISA/210 (second sheet) (July 1998)★